Collusion Resistive Framework For Multimedia Security

Deepak Shukla

Department of Computer Science and Engineering
National Institute of Technology Rourkela

Collusion Resistive Framework For Multimedia Security

Dissertation submitted in partial fulfillment

of the requirements of the degree of

Master Of Technology

in

Computer Science and Engineering

by

Deepak Shukla

(Roll Number: 214CS2157)

based on research carried out

under the supervision of

Prof. Ruchira Naskar

May, 2016

Department of Computer Science and Engineering
National Institute of Technology Rourkela

Department of Computer Science and Engineering
National Institute of Technology Rourkela

Prof. Ruchira Naskar
Assistant Professor

May 10, 2016

Supervisor's Certificate

This is to certify that the work presented in the dissertation entitled *Collusion Resistive Framework For Multimedia Security* submitted by *Deepak Shukla*, Roll Number 214CS2157, is a record of original research carried out by him under my supervision and guidance in partial fulfillment of the requirements of the degree of *Master Of Technology* in *Department of Computer Science and Engineering*. Neither this dissertation nor any part of it has been submitted earlier for any degree or diploma to any institute or university in India or abroad.

_____
Ruchira Naskar

Dedication

Dedicated to my beloved parents and sisters …

Declaration of Originality

I, *Deepak Shukla*, Roll Number *214CS2157* hereby declare that this dissertation entitled *Collusion Resistive Framework For Multimedia Security* presents my original work carried out as a postgraduate student of NIT Rourkela and, to the best of my knowledge, contains no material previously published or written by another person, nor any material presented by me for the award of any degree or diploma of NIT Rourkela or any other institution. Any contribution made to this research by others, with whom I have worked at NIT Rourkela or elsewhere, is explicitly acknowledged in the dissertation. Works of other authors cited in this dissertation have been duly acknowledged under the sections "Reference" or "Bibliography". I have also submitted my original research records to the scrutiny committee for evaluation of my dissertation.

I am fully aware that in case of any non-compliance detected in future, the Senate of NIT Rourkela may withdraw the degree awarded to me on the basis of the present dissertation.

May 10, 2016
NIT Rourkela

Deepak Shukla

Acknowledgment

As a matter of first importance, I would need to express my true regard and thanks towards my supervisor **Dr. Ruchira Naskar**, who has been the controlling light behind this work. I need to recognize her for acquainting me with the energizing field of Multimedia Security and giving me the chance to work under his direction. Her unified confidence in this point and capacity to draw out the best of expository and down to earth abilities in individuals has been priceless in intense periods. Without her priceless recommendations and ever prepared help it wouldn't have been feasible for me to finish this postulation. I am amazingly lucky to have a opportunity to work nearby such a great individual.

I express my appreciation towards all the employees of the CSE Department for their thoughtful collaboration.

When I glance back at my achievements in life, I can see a reasonable hint of my family's concerns and dedication all over the place. My dearest mother, whom I owe all that I have accomplished and whatever I have turned into; my dearest father, for continually trusting in me what's more, moving me to think ambitiously even at the hardest snippets of my life; and my sister who were forever my quiet backing amid every one of the hardships of this attempt and past.

April 20, 2016 — *Deepak Shukla*

NIT Rourkela — Roll Number: 214CS2157

Abstract

The recent advances in multimedia and Internet technology rises the need for multimedia security. The frequent distribution of multimedia content can cause security breach and violate copyright protection law. The legitimate user can come together to generate illegitimate copy to use it for unintended purpose. The most effective such kind of attack is collusion, involve group of user to contribute with their copies of content to generate a new copy. Fingerprinting,a unique mark is embedded have one to one corresponds with user, is the solution to tackle collusion attack problem. A colluder involve in collusion leaves its trace in alter copy, so the effectiveness of mounting a successful attack lies in how effectively a colluder alter the image by leaving minimum trace. A framework,step by step procedure to tackle collusion attack, involves fingerprint generation and embedding. Various fingerprint generation and embedding techniques are used to make collusion resistive framework effective. Spread spectrum embedding with coded modulation is most effective framework to tackle collusion attack problem. The spread spectrum framework shows high collusion resistant and traceability but it can be attacked with some special collusion attack like interleaving attack and combination of average attack. Various attacks have different post effect on multimedia in different domains. The thesis provide a detail analysis of various collusion attack in different domains which serve as basis for designing the framework to resist collusion. Various statistical and experimental results are drawn to show the behavior of collusion attack. The thesis also proposed a framework here uses modified ECC coded fingerprint for generation and robust watermarking embedding using wave atom. The system shows high collusion resistance against various attack. Various experiments are are drawn for the system to shows that the system is highly collusion resistance and have much better performance than other existing literature system.

***Keywords*: *Collusion Attack*; *Interleaving ECC Embedding*; *Wave atom*; *Multiple description*.**

Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Overview

Collusion Resistant Framework (CRF) for multimedia ensure the copyright law for multimedia content against the most popular collusion attack (CA). Copyright law include rights for reproduction, communication, adaption and translation of work to the creator of content. Framework enables the user to use the generated multimedia content in its intended way as supposed by the copyrighter of content. It concern with the security of creator's copyright law, authenticity of content to distributor, genuineness of content to user.

Collusion Attack are become more feasible due to proliferation of digitized media and remote access of user. Collusion Attack involves multiple user to use there legitimate copy of digitized content and perform various static operation on these copies to generate the new copy of content against the copyright law which can be used for illegitimate purpose. Collusion attack are very efficient kind of attack and have too low back tracing rate for colluder as each user contribute equal amount of effort in creation of illegitimate content.

Collusion attack can be avoided with the use of digital fingerprint for multimedia. Digital fingerprint are embed as the information to the content which ensures the identity of user. A digital fingerprint differs from watermark in such a way that fingerprint are embed as the information related to user authenticity while watermark embed the information that is independent of user. A digital watermark is same for various copies of digitized content whereas fingerprint copies of various image is different for various user. So watermark lacks the back tracing property for collusion attack because various colluder has same identical copies can break watermark whereas fingerprint allow to trace up to colluder because each colluder has a unique copy of digitized media.

CRF specifies a series of step to embed the fingerprint to digitized content to avoid the CA. In this thesis, collusion resistant framework uses robust fingerprint embedding based on wave atom transform and multiple description coding. The fingerprints generation fallows ECC(Error correcting code) using Reed Solomon Code.

1.1.1 Anatomy of Collusion Resistant Framework (CRF)

Collusion Resistant Framework defines series of step for multimedia content to avoid the collusion attack on multimedia. It involves preprocessing of multimedia content to make it suitable to embed the fingerprint, embedding of fingerprint, postprocessing the content to convert it into fingerprinted image.

Preprocessing of multimedia content depends upon types of embedding used for fingerprinting. It involves processing to make it compatible for embedding process.

Embedding of multimedia fingerprint involves operations between block of content and fingerprint to produce fingerprinted blocks.

Postprocessing involves the combining the fingerprinted blocks in specified manner to form the fingerprinted content.

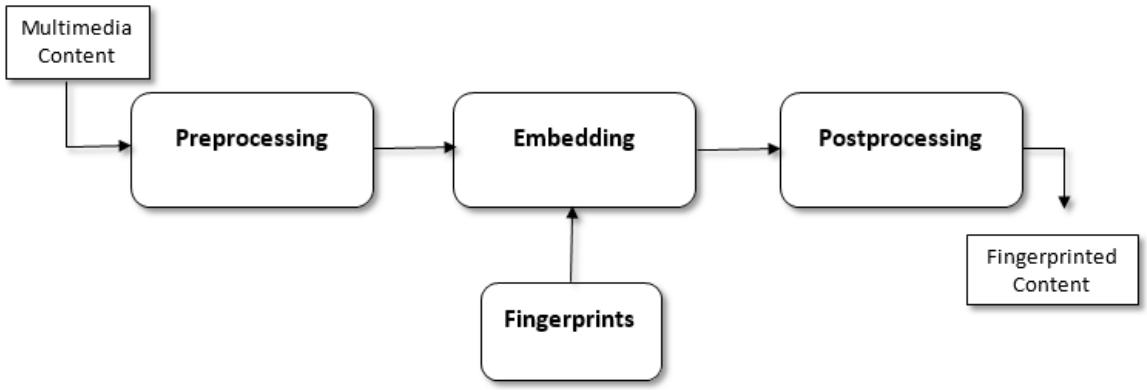
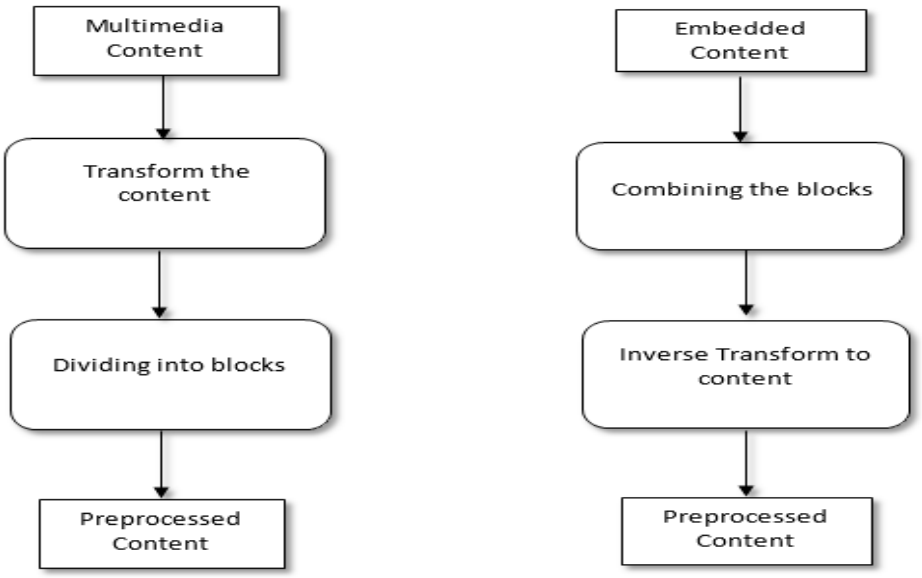


Figure 1.1: Collusion Resistant Framework

Fig. 1.1 shows the pictorial representation for collusion resistant framework. It shows the basic multimedia content is input to system which consist of series of step namely preprocessing, embedding, postprocessing and output the fingerprinted content. The framework assume that fingerprints to embed are present in advance which is input to the embedding step.

Figure 1.2a , 1.2b shows the detailed description of block collusion resistant system. Figure 1.2a shows the preprocessing block of CRF. The block take multimedia content as input and gives preprocessed content as output which is suitable for embedding block. The inner step of block mainly involves transform the content and dividing the blocks. The transform domain and block formation depends upon type of embedding mechanism used for the framework. Figure 1.2b shows the postprocessing block of framework. The block takes embedded content as input and generates fingerprinted content as output. The inner step are just reverse of the steps of postprocessing blocks. The steps involved combining of the blocks to form as original segment and applying inverse transformation to revert back the content to its original domain.



(a) Preprocessing Block (b) Post processing Block

Figure 1.2: Blocks for Collusion Resistance Framework

1.1.2 Digital Fingerprinting Embedding

Embedding digital fingerprint involves encapsulation of fingerprint with multimedia. Embedding fingerprint for multimedia must be robust in manner such that fingerprint can not be removed easily for multimedia content otherwise it become very easy to generate the illegitimate copy of content. Embedding mainly is mapping the generated fingerprints and concatenating them with the transformed multimedia content.

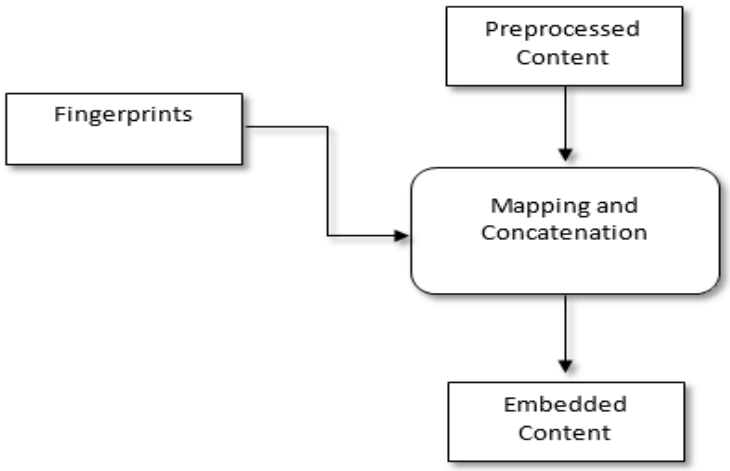


Figure 1.3: Digital Fingerprint embedding

Figure 1.3 shows the block diagram for embedding the fingerprints for CRF. The

embedding procedure takes preprocessed content generated in preprocessing block of CRF as shown in fig 1.2a along with generated fingerprints. The fingerprints are mapped and suitable operation are applied based on CRF to generate the embedded content.

Embedding Techniques

Embedding deals with the robustness of digitized media. The fingerprint embedded in the media is robust from removal that is it can't be isolated from media content otherwise mounting of attack can be done easily. The first data embedding is spread spectrum embedding. Another efficient embedding method which is used in this thesis is robust embedding using wave atom.

Spread spectrum embedding is motivated from spread spectrum modulation technique of signal transmission. Spread spectrum embedding consist of four step as fallow:-

- Selection of feature signal
- Generation of Watermark signal
- Add watermark to feature signal
- Replace Original Feature signal with watermarked one.

Robust Embedding Using Wave Atom uses multiple description coding and wave atom transform. Robust Embedding is as fallow:-

- Make description based on multiple description coding.
- Apply the wave atom transform to the description.
- Select embedding coefficient
- Embedding the coefficient.
- Apply reverse wave atom transform.
- Add the description to form original image.

A detailed description for Robust Embedding Using Wave atom is given in Chapter 4.

1.2 Digital Fingerprinting for Multimedia

Digital fingerprinting (DF) of multimedia involves embedding the piece of information which uniquely identify the user of media to which it is distributed. Fingerprints differs from watermark in a such way that watermark provide genuineness of media content whereas fingerprint provides authenticity for legitimate user.

1.2.1 Issue Related to Digital Fingerprint

DF for multimedia provide legitimacy to user so also faces some issue. The most common issue is to withstand against the removal of fingerprints another is uniqueness for user.

Robustness of DF involve that it cannot be removed from digital media. The more robust is the fingerprint more is the efficiency of fingerprint. Robustness of digital media is achieved by various data embedding method.

Uniqueness implies uniquely identify the user. Fingerprinted generated for the particular user is only correspond to that user. The uniqueness ensures traceability for DF. If a colluder involves in trespassing with its own copy of legitimate media then it leaves some trace in colluded copy which is unique, leads to traceability for that colluder.

Dimension Dependency implies that DF can be generated from user is limited to dimension of code used for generation. So for high number of user the fingerprints must have high dimension. This problem generally occurs for code with no correlation between the fingerprints which can be avoided by adding some means of correlation between the fingerprint.

1.2.2 Fingerprinting Techniques

Fingerprinting Techniques

Fingerprinting deals with generation of uniquely user identifiable fingerprint. The two most widely used fingerprinting mechanism are orthogonal fingerprinting and coded fingerprinting.

Orthogonal Fingerprinting-has stems from orthogonal modulation for signal transmission. It enables watermark to be mutually orthogonal in nature. The orthogonality can be achieved by pseudo random number generator which can generates mutually independent watermark. The orthogonal nature of these watermark allows difference in pattern for multiple user. Orthogonal fingerprint has significantly simple mechanism for embedding and encoding but independency of fingerprint comes at price, it has some drawback:-

- Limited to small group of user.
- Complexity of Detection /traceability is too high
- On linear attack energy reduction is directly dependent upon number of user.
- Fingerprint generation is limited to dimension of fingerprint.

Coded Fingerprinting-uses code modulation technique to construct the fingerprint. Code modulation overcome the drawback of energy reduction and dimensionality limitation. The energy reduction introduced by collusion can be overcome with the correlation so

that positively correlated coefficient of fingerprint do not experience reduction in energy. Correlation can also leads to dependence thus overcome the dimensionality limitation. Coded Fingerprints can be generated in fallowing manner:-

- **Base Code Formation-**to ensure the correlation.
- **Combining the base code with the outer code-**to avoid dimensionality limitation.

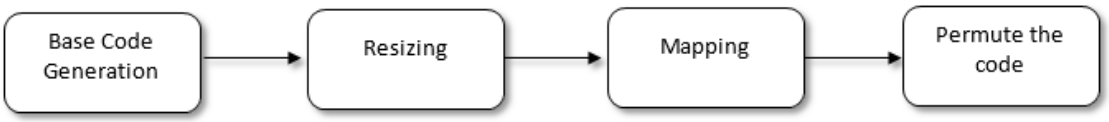


Figure 1.4: Coded Digital Fingerprint

Figure 1.4 gives the scenario for generating the coded fingerprints. It shows the base code generation involve the basic procedure for code generation and depends upon scheme used for coded modulation. The next step in sequence of generation is resizing implies mainly enlargement of base code to match the block dimension of multimedia segment. Next step involve mapping the enlarged code with the predefined code fallowed by arranging the code in sequence to generate the fingerprint.

A detailed description for Coded Fingerprinting is given in Chapter 4.

1.3 Research Motivation

Multimedia Fingerprinting is the core of collusion resistant framework which provide copyright protection and digital right management for the multimedia content. The multimedia fingerprinting can be either independent or correlated that is orthogonal or coded fingerprinting, but has to provide efficient solution to problem of collusion attack. The motivation for this can be listed as fallow:-

- The motive is to model the collusion attack problem such that both image processing attack and collusion attack are taken into account. Also the threshold can be increased for colluder so that optimal solution can be found.
- The problem if solved using orthogonal modulation has drawback of dimension limitation is that the number of user is limited to the dimension of fingerprint. Thus the coded modulation used with robust embedding method in order to provide the solution to the collusion attack problem.

- In real world scenario, the attacker mount collusion attack in different domain (embedding and nonembedding) and also image processing attack. So both efficient fingerprinting and embedding approach must be taken into consideration in order to form optimal solution for collusion resistant framework.

1.4 Problem statement

Collusion attack problem is solved by many researchers. Some has found solution with independent fingerprinting techniques and some with coded fingerprinting techniques with spread spectrum embedding . The primary objective of this research is to provide efficient CRF which is achieved here by providing collusion resistant framework that uses coded fingerprinting with wave atom robust embedding This can be elaborated as fallow:-

- The aim is to use suitable fingerprinting mechanism which intern provide high collusion resistant against the colluder along with the fact that uniqueness property must not be violated. The fingerprinting mechanism must also support the large number of user for system. This leads to find the collusion resistant system with suitable fingerprinting mechanism that provide **uniqueness, dimensional independency**.
- The orthogonal fingerprinting provide uniqueness to system but suffer with dimensional dependency problem so coded fingerprinting are suitable for high number of user. But the simple AND coded fingerprint can be attacked with collusion attack so more efficient coded fingerprint mechanism must be used for optimal system solution.
- The embedding mechanism that are currently in use provide high embedding time for fingerprint so the use of less computational complex mechanism but more secure embedding mechanism require in order to provide optimal system solution.

The design of optimal collusion resistant framework can be achieved by taking fallowing constraints into consideration:

- **Fingerprinting Mechanism** deals with the factor like dimension of fingerprint, number of user. The fingerprints that generates must unique for the system and must not limit with the dimension of code leads to optimal solution.
- **Embedding Mechanism** deals with encapsulation of fingerprinting with the digital content. The strong is the encapsulation more efficient is the embedding mechanism more optimal is the system.
- **Traceability Mechanism** comes in picture after the mounting of the attack. This mechanism deals with the finding the colluder that involves in the collusion. The

traceability mechanism directly dependent upon the types of fingerprinting mechanism used in the system.

1.5 Research Contributions

The research contributes mainly to provide optimal solution to resist the collusion attack problem . The main contribution of thesis is given as fallow:-

- Analysis of various kind of attack that can be mount on the multimedia and provide a statistical measure for different kind of attack in different embedding and non-embedding domain. The analysis of various kind of attack will be helpful in designing the optimal collusion resistant framework.
- The design of efficient collusion resistant framework by providing a novel approach for fingerprint generation and embedding of fingerprint to multimedia. The approach used here uses coded fingerprinting along with robust embedding.

1.6 Thesis Organization

This chapter gives a brief overview of collusion resistive framework. Discussion fallowed digital fingerprinting in multimedia along with techniques and issues related to it.

Chapter 2: A detailed overview for framework is given. The chapter discuss various literature techniques and problem statement is formulated.

Chapter 3: A comparative analysis of various collusion attack on multimedia for coded fingerprint in different domain is given. Chapter discuss the attack model from owner and colluder point of view. Statistical results are drawn for the collusion attack in different domains.

Chapter 4: A detailed description for proposed collusion resistive framework is given. Chapter also discuss the system design process and various simulation parameter.

Chapter 5: Experimental results are drawn for collusion attack in different domains and proposed collusion resistive framework.

Chapter 6: Conclusion for our proposed scheme is given along with future work.

.

Chapter 2

Background and Problem Formulation

2.1 Introduction

Fingerprint generation and embedding are two main building block of optimal collusion resistant system. Fingerprint embedding involves mainly two techniques independent fingerprinting and coded fingerprinting. The independent fingerprint shows high uniqueness whereas cause the problem of dimensional dependency. The orthogonal fingerprint mainly used where number of user are too less are require significant uniqueness and also orthogonal fingerprint are susceptible to collusion attack. *Wu et al.*[1] given a scenario which shows that fingerprints generated using orthogonal modulation are susceptible to linear combination of collusion attack.

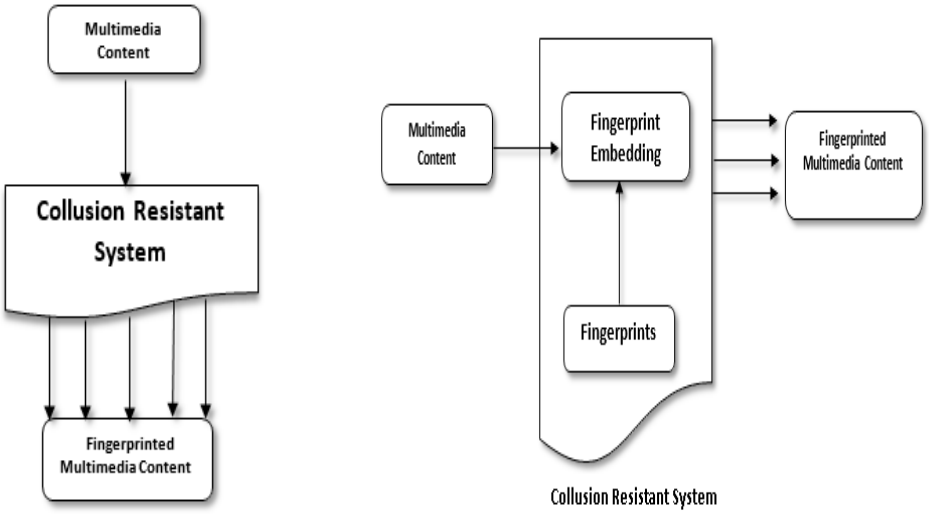
The framework that resist collusion using coded modulation shows more resistibility against the collusion attack. The coded fingerprint techniques generates fingerprint that have some correlation and eliminate the problem of dimensional dependency. In this chapter a detail overview for collusion resistant system is given, also discussion of various collusion resistance system are presented as literature survey. Also various measure are given for collusion resistant system.

2.2 Collusion Resistant System for Multimedia

Fingerprinted content generation mainly involves host signal, collusion resistant system and output fingerprinted multimedia content. A collusion resistant system mainly concatenate fingerprints with host signal. So basically a collusion resistant system is input output system with host signal as input and fingerprinted copies for multiple user as output.

The main aim of fingerprint generation and embedding is to trace back the user which illegally distribute the content against copyright law. The fingerprint generation precedes with some assumption. Orthogonal modulation are based on marking assumption. A orthogonal fingerprint is collection of mark whereas mark is position. The marks are of two types detectable and undetectable. The assumption based on that undetectable mark enchantment leads to meaningless object. So if undetectable mark is changed this will leads

to illegitimate user.



(a) Fingerprinted Content Generation (b) Detailed Collusion Resistant System

Figure 2.1: Collusion Resistive Process

Fingerprinted content generation shown in figure 2.1a 2.1b. A basic block diagram for fingerprinted content generation is shown in Fig. 2.1a. The multimedia content is shown as input to the CRS to generate the fingerprinted content shown as output from the CRS. The basic fingerprinted generation process has three component multimedia content, collusion resistant system and generated fingerprinted content.

Fig. 2.1b shows the detail of collusion resistant system(CRS) along with various component of fingerprint content generation. A CRS has mainly two component fingerprint embedding and fingerprints. Various Fingerprints generated for multiple user and multimedia content are input to fingerprint embedding. The embedding block mainly concatenate or map the fingerprint with host signal to generate fingerprinted copy,unique to every user, depending upon scheme.

2.3 Literary Survey

Collusion Resistant fingerprinting for multimedia is very trendy topic in image processing and many researches are carried out to generate the fingerprint to avoid collusion attack. Various researcher proposed various techniques and framework in order to avoid the collusion attack for multimedia.

Boneh et al. [2] first of all presents a digital fingerprints that can avoid collusion attack. The aim of this work is to give details of code modulation techniques for digital fingerprints. The fingerprinting based on marking and generate unique fingerprint for each of user. *Trappe*

et al. [3] provide a mechanism which uses binary anti collusion code(ACC). The tracing capability of ACC depends upon number of code generated that are uniquely overlapped that the code can trace up only that user for which generated code is uniquely overlapped. *Cox et al.* [4] present a fingerprinting scheme for multimedia content which has it's root from spread spectrum embedding. They states that fingerprint in multimedia content must be placed in appropriate place(must be significant related),enchantment in this leads to degradation in image component. The presented scheme can withstand various signal processing attack as well as collusion attack.

Wu et al. [8] provide forensic analysis for nonlinear collusion attack. Scheme enlighten the detection scenario that can be improved by applying various preprocessing techniques on the media content. The work mainly provides comparison between various non linear attack and their detection strategy according to perceptual quality. *Schonberg et al.* [9] presents digital fingerprinting problem as the analog hole problem. Scheme present a phase shifted collusion resistant scheme. Analysis of collusion resistant for proposed scheme using gradient attack is provided. *Kim et al.* [5] present a scenario for n-secure fingerprinted code. The difference between the watermark and fingerprint along with generation of robust collusion resistant fingerprint is given. Design of code is same for every user and inserted in same position. *Wang et al.* [12] presents forensics for orthogonal modulation. They also derived bound limits for number of colluder to robustness of collusion resistant system. The maximum detector and thresholding detector is used for tracing the user.*Lian et al.* [13] present collusion secure fingerprinting by applying modulation and modulation technique.The scheme assumes distributor as server side to do modulation and user as client side to do demodulation. Modulation is done at server side with pseudo random number and demodulation at client side with fingerprinted code.The demodulation at client side provide source of information that which part of content is being removed and new content is inserted.

Pinkas et al. [6] presented scheme have root from cryptographic scheme which interns leads to colluder when there is large amount of sensitive data is colluded. Author present a probable resilient scheme which is used when user decrypt content above certain threshold. *Tassa et al.* [7] present scenario on dynamic traitor tracing . The work deals with bulk transfer of content and states that there is rights for legitimate user to use the content to ensure this access to the system must be conditional. *Caronni et al.* [10] present a scenario for ownership management of digital image. The work shows the extent to which the fingerprint embed in order to trace the colluder correctly. *Karthik et al.* [11] present digital right management scenario by video fingerprinting and encryption. The main focus is on multi cast communication by presenting a joint secure scheme with encryption and fingerprinting. *Wang et al.* [14] provide a new tree structure detection strategies. They also presents the limit for correlation among the user to identify colluder and give the coded modulation techniques to provide the novel ACC which has property that composition of two or more ACC is unique. The AND code is suitable for antipodal form of fingerprints. *Barg et al.* [15] present

the codes ensure tracing of at least one colluder if collusion occur in the system. The tracing probability of at least one user is $\exp(-\omega(n))$ for coalition of size-t. They also ensures that code generation complexity is polynomial time of number of user.Another method for fingerprinting multimedia data, video, audio presents by [16]. The generated fingerprint are Gaussian random vector. They states that the placement of fingerprint also must be significant so that modification in this portion leads to the destruction of multimedia content. The work also states that placing the fingerprint in particular region makes the fingerprinted copies robust in nature to withstand against the general distortion as well as collusion attack.

Manaf et al. [17] present the framework for collusion resistant in video which focuses on copyright protection. The proposed scheme process video content by frame. The scheme uses block coding along with truncation ,wavelet transformation and decompose the singular value to achieve the robustness and quality. As processing and fingerprint generation is done for each frame so it is computationally hard for attacker to detect the fingerprints. *He et al.* [18] provide video fingerprint for bulk transfer with collusion resistant property. The work consider the real world problem deals with distribution of content TV or DVD which has significantly large number of user in range of 100 million. So this large set of user has highly efficient CRF which has not only have high collusion resistibility but also less computational complexity for tracing and generation complexity for fingerprint. They proposes a mechanism considering both encoding and embedding for coded fingerprint. They shows that coded fingerprint has high detection capacity while lack in resistibility.

Kirovski et al. [27] presents the collusion attack problem as 'analog hole problem'. The analog hole problem states that traditional cryptographic scheme such as encryption can't apply for protection of multimedia content. The work explore the issue and the solution to proposed problem along with analysis of various classes of spread spectrum embedding namely direct ,uniform and bounded Gaussian distribution. *Kuribayashi et al.* [19] propose a fingerprinting scheme based on Code Detection Multiple Access Technique (CDMA). The fingerprint generation fallows DCT transform along with pseudo noise sequence. A hierarchical manner is fallowed for increasing the number of fingerprinted code. The fingerprints are made up of group number and user number. For detection of colluder FDCT algorithm is used which significantly reduces the detection complexity. *Schaathun et al.* [30] presents the counter attack to the [19]. The author claims that the scheme is susceptible to non-linear collusion attack. The author defines two novel attack using conventional attack that is moderated minority extreme attack,the attack is limiting function of minimum and maximum attack and uniform attack,perform attack at regular interval of range and is combination of maximum and midpoint attack. *Hernandez et al.* [20] test the effectiveness of [19]. They check the robustness of scheme against collusion attack along with perceptual transparency for scheme. They investigate the scheme by giving upper bound of distortion for fingerprints. Results shows that scheme suited well for real world application belongs to restricted distribution of content.

Cha et al. [21] proposes scheme against time varying collusion attack. They proposed the MC-CDMA system and gives scheme to improve the efficiency of system. The work focuses on audio signal proceeds by making of auditory system based on characterization and noticeable difference. They provide advance detector and interleaving coding as solution to problem of collusion attack. The work discuss interference in collusion attack and also focuses on dynamics of same. *Qureshi et al.* [22] provide a framework for content distribution for preserving security and privacy which focuses on peer to peer network. The end user is private in network whereas the merchant owns copyright law so that a strong copyright mechanism must be employed in the system that deals with both privacy issue and copyright enforcement. The framework ensures colluder tracing,buyer authenticity and collusion resistant.

Zhao et al. [23] presented various statistical measures related to linear and nonlinear collusion attack. They work is solely based on independent fingerprint. They also gives the importance of perceptual quality and collusion resistant of fingerprint. The work also suggest bounding the Gaussian fingerprint as a solution to improve the quality and lower the distortion of generated fingerprinted content along with covenant between the collusion attack and quality of output fingerprinted content. *Li et al.* [24] gives comparison for various linear and non-linear attack in embedding and non-embedding domain. The work provide model of collusion attack from the owner and colluder point of view as the owner deals with certain component of content whereas the colluder deals the component as whole so two different model are required. They also discuss the covenant between the image quality and collusion attack. [1] presents a novel attack on multimedia known as Linear Combination Of Collusion attack(LCCA),a generic average attack. LCCA generate the colluded copy of good quality along with hardening the tracing for system. The work check the strength of AND-ACC code presnted by *Trappe et al.* [3] ,who claims that AND-ACC can resist the average collusion attack. However they shows that AND-ACC coded fingeprints can be easily attacked with LCCA leaving no trace. *Wang et al.* [25] present various statistical measures and analysis on non-linear collusion attack. The work solely based on orthogonal Gaussian fingerprints. They suggest that unbounded Gaussian fingerprint have some kind of distortion in the output content,whereas bounded Gaussian fingerprint provide image of good quality. *Doerr et al.* [26] presents the collusion attack on video using mosaicing,all video are processed to have same constraint. The collusion attack here is intra video collusion attack,which assumes watermarking video is the watermarking multiple still images. For video if same watermark is applied to different frame then the collusion attack extract watermark from images and subtract it to watermark content to get original content.*Wu et al.* [28] presents a novel attack on watermarking scheme considering buyer authentication. The buyer authentication scheme perform modification on certain pixels depending on secret key information. The collusion attack present here is adaptive to situation in which the colluder chooses certain pixel of output content and perform average on these pixel to remove the

authentication information. *Etesami et al.* [29] proposes a collusion attack on fingerprints generated from finite alphabet.The attack is non-linear in nature perform statistical operation maximum and multiplication(π) on fingerprints. The work discuses the correctness of attack for various random and deterministic schemes along with providing lower bound for number of colluder. *Li et al.* [24] has also given same analysis for collusion attack using Gaussian fingerprint. They proposes the two different attack model from owner and colluder point of view. The two model are different in nature because colluder uses all component of multimedia content to attack while owner uses only partial component. So for analyzing collusion attack effectively it is mandatory to use different collusion attack model from that of owner model for attack.

Zheng et al. [31] proposed modified traceable code scheme , which is Interleaving embedding scheme(ILE). ILE scheme enforces the interleaving of various block of fingerprint before embedding. ILE scheme increases the collusion resistive ability of codes. They found that if every conspirator contribute same to the colluded content then colluder identification will become more feasible. ILE scheme uses the same fact ,a hidden key is used for permutation of interleaved fingerprints. *He et al.* [18] study the performance of error correcting codes(ECC). The ECC are much more traceable code than resistive. The study concern with both coding and embedding issue. They shown that average attack is best attack to mount on independent fingerprint while in ECC it has no significant. *Cheng et al.* [32] investigates collusion codes and various algorithm. The investigation carried out for traditional AND-Anti collusion code(AND-ACC). They found that there exist various other logical code which has better performance than AND-ACC. The new collusion code logical Anti collusive code and various algorithm for detecting the collusion is obtain.*Leung et al.* [33] proposed a robust embedding scheme for watermarking the image. The scheme interns uses wave atom domain for embedding the mark into content. The scheme is based on blind watermarking that is the watermark extraction does not need original content. The comparative analysis between element gives the watermark. The original signal is divided into five scale band signal out of which one is used to insert the mark.

Koubaa et al. [34] proposed the watermarking scheme for video which can resist collusion attack along with several video processing attack. The scheme uses mosaicing,which is creating a larger content from some small correlated content. Mosaicing finds the area of interest in which the marking should be done. The scheme uses here finds correlated area which interns embedded with same mark every time. The scheme lacks that embedded mark can not be detect only it is inserted or not can be identified. *Boroujerdizadeh et al.* [35] proposes a method which diminishes the occurrence of attack in watermark. The work is related to video watermarking. The scheme is based upon conventional method used in cryptography which is key management. They assume that collusion attack arises by exchanging the files between the user,so that roper key management can reduce the problem of collusion. The assume that to fully eliminate the attack one key for every user is used

in the system. *Tirkel et al.* [36] proposes the fingerprinting scheme for audio which resist the collusion. The audio signal must be protected with fingerprints as the transceivers may drop some signal which intern used by the colluder. A vector space is formed with the help of principal component. The fingerprints are assumed as rotation in that space in ordered manner. The rotation is represented with sequence of related properties. These related sequence array are inserted into audio which are collusion resistive. *Maity et al.* [37] proposes a optimization in spread spectrum watermarking which interns resist fading like collusion. The framework is based on genetic algorithm which uses wavelet domains. The wavelet decomposition is multiband in nature is assets for space and energy. The use of M-band makes the scheme robust against fading. The genetic algorithm are used to generates the watermark by selecting suitable threshold. The scheme used a function based on original content ,robustness and embedding imperceptibility.

2.4 Problem Formulation

There are N user for collusion resistant multimedia system with multimedia content is represented by M has length N. The system generates a unique fingerprint $f^{(i)}$ also of length N for each user $u^{(i)}$ where $i = 1, 2, 3...N$. The thesis used coded modulation for fingerprint generation so the generated fingerprint for N user $\{W^{(i)}\}_{i=1}^{N}$ has correlation between them. The fingerprinted multimedia content $Y^{(i)}$ is distributed to user.

The fingerprint embedding mechanism used here is robust embedding using wave atom[33]. So the based on [33] multiple description coding is used for multimedia content before embedding the fingerprint . So the content M is divided into four equal sub block upper and lower even odd blocks.

The content M has size $N \times N$. The sub block generation are as fallows-

$$M^1 = M(i, 2j-1),\ M^2 = M(i, 2j)$$
$$M^3 = M(\tfrac{N}{2} + i, 2j-1),\ M^4 = M(\tfrac{N}{2} + i, 2j)$$

where M^1, M^2, M^3, M^4 are the sub block for upper and lower even odd description of multimedia content M and $i = 1, 2, 3...N/2$,$j = 1, 2, 3...N/2$.

The fingerprint for the various sub block is represented by Y.The generation fallows the equation

$$Y_k^{(i)} = M_k^j + \gamma f_k^{(i)} \tag{2.1}$$

.

where $Y_k^{(i)}$, M_k^j, $f_k^{(i)}$ are the kth component of fingeprinted content , kth subblock of content M and fingeprints.

2.4.1 Collusion Attack on Multimedia

It involves multiple user to combine there unique copy of fingerprinted image and generate an illegitimate copy of unique fingerprinted image by applying some statistical method. CA can be merely divided on basis of nature of statistical operation as Linear and Non Linear collusion attack.

Assume that out of N user C are colluder with colluder set $C_s = \{c_{i_1}, c_{i_2}, c_{i_3}...c_{i_c}\}$. The collusion attack involve C different copies of fingerprinted content $\{C^{(i)}\}_{i=1}^{N}$ to generate a colluded copy with kth component as S_k.

Attack Model:-

$$S_k = C(Y_k^{(i)}) \tag{2.2}$$

where C(.) is a collusion function. The attack model for various attack takes fingerprinted copy as input and generates colluded content as output.

Linear collusion attack involves group of colluder with their individual copies of media and they linearly(such as averaging) combine to produce the colluded copy of media. The linear operation are like summation and averaging are performed on group of media.

Linear Collusion Attack:

$$S_k^a vr = g(\frac{Y_k^{(i)}}{C}) \tag{2.3}$$

where g(.) is a linear operation like average or linear combination of average. S_K^{avr} is colluded copy generate by C colluder under average attack and $Y_k^{(i)}$ is kth component fingerprinted copy for ith colluder belong to colluder set C_s

Nonlinear collusion attack differs from linear collusion attack in manner of operation performed on media. Attack perform some nonlinear operation(such as maximum, minimum, median) on the media copies of colluder to generate illegitimate copy of media content.

NLCA are more computationally expensive than linear counterpart in a manner as they require more complex operation on such as comparison for finding maximum and minimum among the media. So LCA attack can be executed more easily is one of the possible reason for popularity and frequently use of LCA.

LCA has one more advantage for colluder over NLCA is that they are less traceable. LCA are less traceable because group of colluder contributed to same extent in generation of colluded copies and linear operation (averaging) also reduces the power of each legitimate fingerprinted copies of media in colluded copy of media. So the LCA can be executed more efficiently if the number of user involve in collusion is high as there is less trace for individuals fingerprints.

System Model equation for Non Linear Collusion Attack are -

Non Linear Collusion Attack:

$$S_k^a vr = g(\frac{Y_k^{(i)}}{C}) \tag{2.4}$$

where g(.) is a non linear operation like minimum,maximum,median etc.If operation is minimum then it is minimum non linear collusion attack,if maximum ,medium then it is maximum ,median collusion attack respectively. S_K^{avr} is colluded copy generate by C colluder under average attack and $Y_k^{(i)}$ is kth component fingerprinted copy for ith colluder belong to colluder set C_s

2.4.2 Performance Measure

The fallowing perform measure are used here to analyze the effectiveness of system.

Perceptual Quality measure the quality for generated fingerprinted multimedia content. The common measure used for generated content are mean square error(MSE) and peek signal to noise ratio(PSNR). But MSE measure has some weakness as it does not account some quality of image also MSE take noise distortion in content as whole does not consideration noise for each component.

So to measure perceptual quality [23] provide an additional measure which is just noticeable difference(JND). The JND can be used as thresold for distortion of content. If the distortion in data values of content is less than JND then there will be not a significant distortion for content.

They define two criteria measure using JND ar as fallow -

- Noise component that exceeds the JND

$$N_{jnd} \equiv \sum_{j=1}^{N} M_{(no_j > jnd_j)}/N; \tag{2.5}$$

- Modified mean square value is

$$MSE_{jnd} \equiv \sum_{j=1}^{N} no_j'^2 \tag{2.6}$$

where no_j' is as fallow

$$\begin{cases} no_j + jnd_j, & if\ no_j < -jnd_j; \\ 0, & if\ -jnd_j \leq no_j < jnd_j; \\ no_j + jnd_j, & if\ no_j < jnd_j; \end{cases} \tag{2.7}$$

A very high value of these measure indicate that the generated fingerprinted image is not of certain standard.

Collusion Attack And Detcetion Effectiveness The performance measure of system model depends upon the success of mounting collusion attack and then tracing the colluder in the system. The mounting success of collusion attack and tracing success of colluder depends upon various criteria according to application. Among the various criteria the most effective criteria are false positive and false negative. False positive here implies tracing to legitimate user and assume it as colluder. False negative criteria is tracing to colluder and ignoring it likewise legitimate user. The measuring for these criteria are-

- P_{doc}:Probability of detecting at least one colluder.
- P_{foc}: false positive probability of system that is falsely detecting at least one colluder.
- N_{ac}: Number of actual colluder in system.
- N_{fn}: False positive fraction of user in system that is number of user that are detected falsely by the system.

These criteria serve as basic for effectiveness of collusion resistant system and which measure is taken into consideration depends upon application domain. Some application make high priority to capturing colluder irrespective of capturing innocent colluder ,for these types of system P_{doc} and P_{foc} are useful. On other hand application where false accusing is crime take N_{ac} and N_{fn} into consideration.

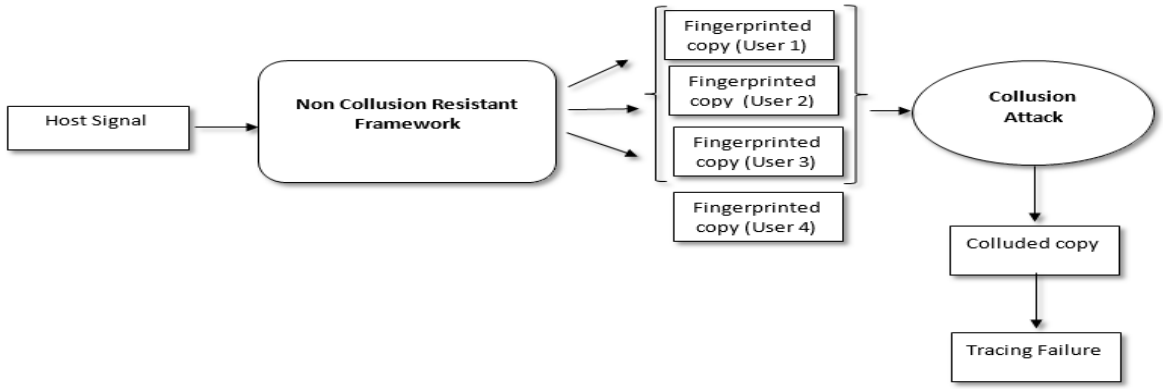
2.4.3 Solution to Collusion Attack Problem

Collusion attack become more feasible and cost effective attack in literature due to advancement in Internet. The colluder can mount attack remotely on multimedia content with its legitimate copy. The attack mounting can be done from any place, various colluder involve in the system can contribute with their fingerprinted copy without being in same place.Likewise generation, distribution of illegitimate content is also simple. The leads to add serious issue to copyright protection. The collusion framework is the solution to collusion attack problems.

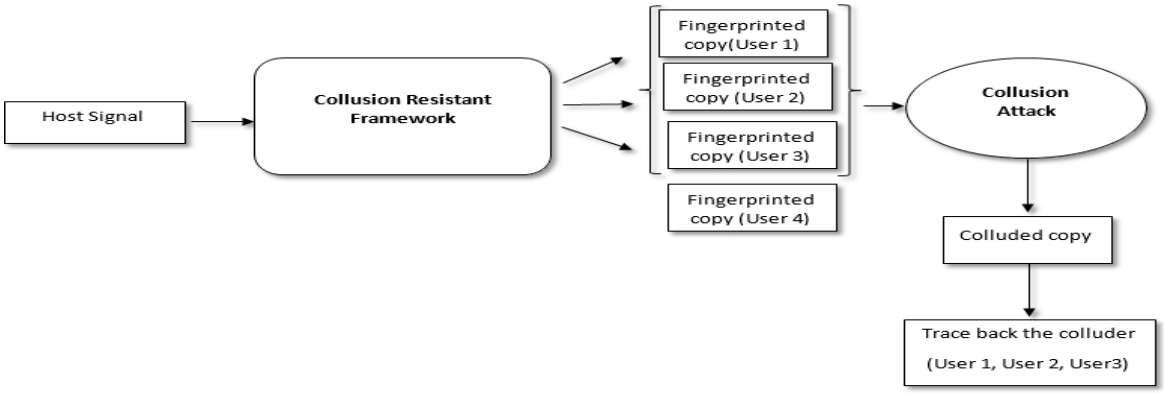
Collusion resistant framework employed in the system to withstand against the collusion attack. The System comprises mainly digital fingerprinting and embedding mechanism. The most commonly used digital fingerprinting mechanism in the literature are orthogonal or independent fingerprint and coded fingerprints.

The orthogonal fingerprints are computationally inexpensive and can generate fingerprint easily as its counterpart coded fingerprint but suitable for small group of user as limited with dimension of code used. So for large number of user coded fingerprint are suitable as they offer some means of correlation between generated fingerprint.

The design of collusion resistant framework differs from non collusion resistant framework. CRF are design in such manner that the colluded copy leads to colluder involve in collusion. The detail of collusion resistant framework is described in Section 2.2. The tracing capability of CRF depends upon the fingerprint generation and assumption made to choose the code.



(a) Non Collusion Resistant Framework



(b) Collusion Resistant Framework

Figure 2.2: Comparison of Non Collusive and Collusive Framework

Figure 2.2a and 2.2b shows the scenario of using non collusion and collusion resistant framework respectively.

Figure 2.2a shows the of using non collusion resistant framework in which a colluder generate colluded copy and be intractable by the system. Figure shows the system generates fingerprinted copy (for simplicity only four copies are generated) out of which three user take participation in collusion to generate colluded copy but due to system framework colluder can't be trace out.

Figure 2.2b shows counter scenario for collusion resistant framework in which system framework is design in such manner that colluded copy leads to colluder. The same three colluder involve in collusion and generate the colluded copy. The system use the colluded

copy to trace back the conspirator.

The tracing capability of system depends upon types of fingerprinting generation mechanism employed. For orthogonal fingerprint it can only trace one user at a time. For coded modulation it depends upon type of base code used for fingerprint construction.

2.5 Conclusion

The chapter discussion starts with a brief overview collusion resistant system. Also the preexisted related work is given as reference to the CRS. The problem structure is also given in details along with the the some performance measure criteria to measure effectiveness of system. The chapter ends with providing solution to collusion attack problem. The next chapter deals with the analysis of different collusion attack in different domains.

Chapter 3

Analysis of Collusion Attacks

3.1 Introduction

Collusion attack very destructive and efficient attack, from colluder point of view, involve a group of user to contribute their individual and legitimate copy of multimedia content, distribute by owner, to generate the colluded copy. Collusion attack significantly decrease the energy signal for colluder involve in the system as it is difficult or nearly impossible to trace back the colluder. Collusion attack mainly divided into two kind depending upon their mode of operation on that is **linear attack** and **non linear attack**.

The analysis of different kind of attack in different domain serve as a basis of designing collusion resistant system. The chapter provide a detail analysis of linear and non-linear attack in DCT, spatial and wavelet domain for coded fingerprint.The chapter start with discussing statistical analysis for attack on coded fingerprinting system fallows by giving image quality after different attack. In end, simulation result are given for domain analysis of attack on coded fingerprint.

3.2 Collusion Attack

Collusion attack are mainly divided into linear and non-linear collusion attack. The most popularly used linear collusion attack is average attack. The non linear attack can be of different kind depending upon the operation performed on multimedia. The various non linear operation include minimum,maximum,median,combination of minimum maximum,combination of all there minimum,maximum and median attack,combination of minimum and maximum with some probability.

Assume the original multimedia content vector is M has length N. There are L fingerprint system denoted by $\{f_j^{(k)}\}_{j=1}^{L}$. The fingerprint generation fallows the equation

$$Y_j^{(k)} = X_k + \gamma f_j^{(k)} \tag{3.1}$$

where the Y_j^k is kth component of fingerprinted copy distributed to jth user, γ is experimental

constant and $f_j^{(k)}$ is kth component of fingerprint for jth user. The C out of N user are colluder with the colluder set $C_s = \{1, 2, 3...C\}$.

3.2.1 Types of Collusion Attack

Linear Collusion Attack

They are the most widely used and effective attack for multimedia.The average attack is one of the attack involve linear operation on the fingerprinted copy of content.

Average Attack:

$$S_i^{avr} = (\sum_{i \epsilon C_s} \frac{Y_i^{(k)}}{C}) \tag{3.2}$$

Non-linear Collusion Attack

They can be of different type depending upon number of operation that can be performed on content. The non linear collusion attack are as fallow-

Minimum Attack:

$$S_i^{min} = min(\{Y_k^{(i)}\}_{k \epsilon C_s}) \tag{3.3}$$

Maximum Attack:

$$S_i^{max} = max(\{Y_k^{(i)}\}_{k \epsilon C_s}) \tag{3.4}$$

Median Attack:

$$S_i^{med} = median(\{Y_k^{(i)}\}_{k \epsilon C_s}) \tag{3.5}$$

Minmax Attack:

$$S_i^{minmax} = \frac{min(\{Y_k^{(i)}\}_{k \epsilon C_s}) + max(\{Y_k^{(i)}\}_{k \epsilon C_s})}{2} \tag{3.6}$$

Modneg Attack:

$$S_i^{modneg} = min(\{Y_k^{(i)}\}_{k \epsilon C_s}) + max(\{Y_k^{(i)}\}_{k \epsilon C_s}) - median(\{Y_k^{(i)}\}_{k \epsilon C_s}) \tag{3.7}$$

Randneg Attack:

$$S_i^{rndmneg} = \begin{cases} mein(\{Y_k^{(i)}\}_{k \epsilon C_s}) & \text{with probabilty p} \\ max(\{Y_k^{(i)}\}_{k \epsilon C_s}) & \text{with probabilty 1-p} \end{cases} \tag{3.8}$$

where S_i^{avr},S_i^{min},S_i^{max},S_i^{med},S_i^{minmax},S_i^{modneg}, $S_i^{rndmneg}$ are the colluded copy generated form average attack,minimum attack,maximum attack ,minmax attack ,modneg attack,rndmneg attack respectively. The function min(.),max(.),median(.) represent statics

minimum,maximum and median operation. $Y_k^{(i)}$ is the fingerprinted copy as per Equation 3.1. C is number of colluder with C_s as colluder set ,p is probability constant.

3.2.2 Owner Attack Model

It take consider for partial component is as fallow-

Average Attack:

$$S_i^{avr} = (\sum_{i \epsilon C_s} \frac{Y_i^{(k)}}{C})$$

Minimum Attack:

$$S_i^{min} = min(\{Y_k^{(i)}\}_{k \epsilon C_s})$$

Maximum Attack:

$$S_i^{max} = max(\{Y_k^{(i)}\}_{k \epsilon C_s}) \tag{3.9}$$

Median Attack:

$$S_i^{med} = median(\{Y_k^{(i)}\}_{k \epsilon C_s})$$

Minmax Attack:

$$S_i^{minmax} = \frac{min(\{Y_k^{(i)}\}_{k \epsilon C_s}) + max(\{Y_k^{(i)}\}_{k \epsilon C_s})}{2}$$

Modneg Attack:

$$S_i^{modneg} = min(\{Y_k^{(i)}\}_{k \epsilon C_s}) + max(\{Y_k^{(i)}\}_{k \epsilon C_s}) - median(\{Y_k^{(i)}\}_{k \epsilon C_s})$$

Randneg Attack:

$$S_i^{rndmneg} = \begin{cases} min(\{Y_k^{(i)}\}_{k \epsilon C_s}) & \text{with probabilty p} \\ max(\{Y_k^{(i)}\}_{k \epsilon C_s}) & \text{with probabilty 1-p} \end{cases}$$

3.2.3 Colluder Attack Model

It consider the blind attack as colluder have no information about coefficient of multimedia content so collude over all coefficient involve. So the model for colluder is as of owner with slight changes are as fallow-

Average Attack:

$$S_i^{avr} = (\sum_{i \epsilon C_s} \frac{Y(i,j)}{C})$$

Minimum Attack:

$$S_i^{min} = min(\{Y(i,j)\}_{k \epsilon C_s})$$

Maximum Attack:

$$S_i^{max} = max(\{Y(i,j)\}_{k \epsilon C_s}) \tag{3.10}$$

Median Attack:

$$S_i^{med} = median(\{Y(i,j)\}_{k \epsilon C_s})$$

Minmax Attack:

$$S_i^{minmax} = \frac{min(\{Y(i,j)\}_{k \epsilon C_s}) + max(\{Y(i,j)\}_{k \epsilon C_s})}{2}$$

Modneg Attack:

$$S_i^{modneg} = min(\{Y(i,j)\}_{k \epsilon C_s}) + max(\{Y(i,j)\}_{k \epsilon C_s}) - median(\{Y(i,j)\}_{k \epsilon C_s})$$

Randneg Attack:

$$S_i^{rndmneg} = \begin{cases} min(\{Y(i,j)\}_{k \epsilon C_s}) & \text{with probabilty p} \\ max(\{Y(i,j)\}_{k \epsilon C_s}) & \text{with probabilty 1-p} \end{cases}$$

3.3 Embedding and Non-embedding Domain

The most of the literature assumes DCT domain as embedding domain and spatial ,wavelet domain as non embedding domain. The domain differs in manner of transformation applied on fingerprinted content.

- The embedding domain(DCT domain) perform discrete cosine transformation on fingerprints fallowed by collusion attack
- The spatial domain perform DCT, IDCT on fingerprints fallowed by collusion attack.
- The wavelet transformation perform DWT operation alongwith DCT, IDCT

Figure 3.1: Collusion Attack in Embedding DCT Domain

Figure 3.1, 3.2, 3.3 shows the block diagram for collusion attack in different domains.

Figure 3.2: Collusion Attack in Non-Embedding Spatial Domain

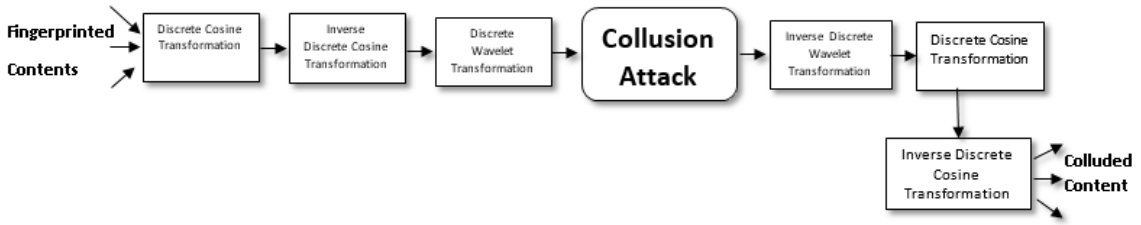


Figure 3.3: Collusion Attack in Non-Embedding Wavelet Domain

- Figure 3.1 shows the collusion attack on fingerprinted copy in embedding(DCT) domain. The discrete cosine transformation(DCOT) is applied on the fingerprinted copy of multimedia content which fallows collusion operation. The inverse discrete cosine transformation(IDCOT) is also applied to revert back to content to its original domain that will generate the colluded image.

- Figure 3.2 shows the collusion attack procedure in non-embedding(spatial domain)domain. The attack added one extra DCOT operation from **??**. The fingerprinted image first operate with $DCOT_1$ and $IDCOT_2$ on which collusion is perform which fallowed by $DCOT_2$ for first $IDCOT_2$ and $IDCOT_1$ operation for corresponding $DCOT_1$ to revert back it to original domain which intern generates original image. The subscript used here to show correspondence.

- Figure 3.3 shows the collusion attack procedure in non-embedding(wavelet domain)domain. The procedure added one extra discrete wavelet operation(DWOT) than spatial domain transformation. The process perform $DCOT_1$,$IDCOT_2$,$DWOT$ operation on fingerprinted image in manner on which the collusion attack is performed which fallowed $IDWT$,$DCOT_2$,$IDCOT_1$ in manner to generates the colluded copy.

3.4 Statistical Analysis

The testing to collusion by owner and collusion attack by colluder differs in processing as they both treats multimedia content differently. The owner only collude with partial

component to check the effectives of system whereas colluder collude blindly with the content. So to check the effectiveness of collusion attack both types of system model is taken into consideration.

3.4.1 Collusion Attack Model

Suppose Y_k is output fingerprinted content produce by equation

$$Y_{(k)} = X_k + \gamma f_{(k)} \tag{3.11}$$

with colluder set C_s. So Y_k to which operation C(.) is performed with $k \epsilon C_s$ where C(.) is collusion attack operation.

- Collusion Attack In Domains
  - Embedding Domain(DCOT Domain)

$$CollusionAttack_{DCOT} = C(Y_k) \tag{3.12}$$

  - Non-Embedding Domain(Spatial Domain)

$$CollusionAttack_{spatial} = DCOT(C(DOCT^{-1}(Y_k))) \tag{3.13}$$

  - Non-Embedding Domain(Wavelet Domain)

$$CollusionAttack_{wavelet} = DCOT(DWT_{-1}C(DWT(DOCT^{-1}(Y_k)))) \tag{3.14}$$

where $DCOT$,$DCOT^{-1}$,$DOWT$,$DOWT^{-1}$ are discrete cosine transformation ,inverse discrete cosine transformation,discrete wavelet transformation,inverse discrete wavelet transformation respectively.

Some convention in operation is used for comparison of attack.

- Attack M >Attack N implies attack M is overperform to attack N in attacking the coded fingerprint.
- Attack M $\approx$ Attack N implies attack M and attack N has similar effect in attacking the coded fingerprint.
- Attack M=Attack N implies attack M and attack N has same effect in attacking the coded fingerprint.

3.4.2 Attack Performance in Different Domains

- **Average Collusion Attack** is linear operation.
  - Embedding Domain(DCOT Domain)

$$CollusionAttack_{DCOT}^{average} = A(Y_k) \tag{3.15}$$

  - Non-Embedding Domain(Spatial Domain)

$$\begin{aligned} CollusionAttack_{spatial}^{average} &= DCOT(A(DOCT^{-1}(Y_k))) \\ &= DCOT(DCOT^{-1}A(Y_k)) \\ &= A(Y_k) \end{aligned} \tag{3.16}$$

  - Non-Embedding Domain(Wavelet Domain)

$$\begin{aligned} CollusionAttack_{wavelet}^{average} &= DCOT(DWT_{-1}A(DWT(DOCT^{-1}(Y_k)))) \\ &= DCOT(DWT_{-1}(DWT(DOCT^{-1}A(Y_k)))) \\ &= A(Y_k) \end{aligned} \tag{3.17}$$

where $CollusionAttack_{DCOT}^{average}$,$CollusionAttack_{spatial}^{average}$,$CollusionAttack_{wavelet}^{average}$ are the average collusion attack in embedding(DCOT) domain,spatial domain,wavelet domain.A(.) is the average operation on fingerprints. The Equation 3.16, 3.17 conclude that average attack is domain independent.

$$\mathbf{CollusionAttack_{DCOT}^{average} = CollusionAttack_{spatial}^{average} = CollusionAttack_{wavelet}^{average}} \tag{3.18}$$

- **Random negation Attack** is, combination of minimum and maximum attack, non linear operation. The attack has dual behavior for let p probability it is maximum attack and (1-p) it is minimum attack.
  - Embedding Domain(DCOT Domain)

$$CollusionAttack_{DCOT}^{rndmneg} = R(Y_k) \tag{3.19}$$

  - Non-Embedding Domain(Spatial Domain)

$$CollusionAttack_{spatial}^{rndmneg} = DCOT(R(DOCT^{-1}(Y_k))) \tag{3.20}$$

– Non-Embedding Domain(Wavelet Domain)

$$CollusionAttack_{wavelet}^{rndmneg} = DCOT(DWT_{-1}R(DWT(DOCT^{-1}(Y_k)))) \tag{3.21}$$

where $CollusionAttack_{DCOT}^{rndmneg}$,$CollusionAttack_{spatial}^{rndmneg}$,$CollusionAttack_{wavelet}^{rndmneg}$ are the average collusion attack in embedding(DCOT) domain,spatial domain,wavelet domain.R(.) is the random negation operation on fingerprints.

- **Minimum Collusion Attack** is non linear operation.

  – Embedding Domain(DCOT Domain)

$$CollusionAttack_{DCOT}^{minimum} = Min(Y_k) \tag{3.22}$$

  – Non-Embedding Domain(Spatial Domain)

$$\begin{aligned} CollusionAttack_{spatial}^{mimimum} &= DCOT(Min(DOCT^{-1}(Y_k))) \\ &< DCOT(DCOT^{-1}Min(Y_k)) \\ &= Min(Y_k) \end{aligned} \tag{3.23}$$

  – Non-Embedding Domain(Wavelet Domain)

$$\begin{aligned} CollusionAttack_{wavelet}^{minimum} &= DCOT(DWT_{-1}Min(DWT(DOCT^{-1}(Y_k)))) \\ &< DCOT(DWT_{-1}(DWT(DOCT^{-1}Min(Y_k)))) \\ &= Min(Y_k) \end{aligned} \tag{3.24}$$

where $CollusionAttack_{DCOT}^{minimum}$,$CollusionAttack_{spatial}^{minimum}$,$CollusionAttack_{wavelet}^{minimum}$ are the minimum collusion attack in embedding(DCOT) domain,spatial domain,wavelet domain.Min(.) is the minimum operation on fingerprints. The Equation 3.23,3.24 conclude that minimum attack perform differently in different domains.

$$\mathbf{CollusionAttack_{DCOT}^{minimum} > CollusionAttack_{spatial}^{minimum} > CollusionAttack_{wavelet}^{minimum}} \tag{3.25}$$

- **Maximum Collusion Attack** is non linear operation.

  – Embedding Domain(DCOT Domain)

$$CollusionAttack_{DCOT}^{maximum} = Max(Y_k) \tag{3.26}$$

– Non-Embedding Domain(Spatial Domain)

$$\begin{aligned} CollusionAttack_{spatial}^{maximum} &= DCOT(Max(DOCT^{-1}(Y_k))) \\ &< DCOT(DCOT^{-1}Max(Y_k)) \\ &= Max(Y_k) \end{aligned} \tag{3.27}$$

– Non-Embedding Domain(Wavelet Domain)

$$\begin{aligned} CollusionAttack_{wavelet}^{maximum} &= DCOT(DWT_{-1}Max(DWT(DOCT^{-1}(Y_k)))) \\ &< DCOT(DWT_{-1}(DWT(DOCT^{-1}Max(Y_k)))) \\ &= Max(Y_k) \end{aligned} \tag{3.28}$$

where $CollusionAttack_{DCOT}^{maximum}$,$CollusionAttack_{spatial}^{maximum}$,$CollusionAttack_{wavelet}^{maximum}$ are the minimum collusion attack in embedding(DCOT) domain,spatial domain,wavelet domain.Max(.) is the maximum operation on fingerprints. The Equation 3.27,3.28 conclude that maximum attack perform differently in different domains.

- **Maxmin Collusion Attack** is ,average operation perform over minimum and maximum attack,non linear operation.

  – Embedding Domain(DCOT Domain)

$$CollusionAttack_{DCOT}^{maxmin} = Maxmin(Y_k) \tag{3.29}$$

  – Non-Embedding Domain(Spatial Domain)

$$\begin{aligned} CollusionAttack_{spatial}^{maxmin} &= DCOT(Maxmin(DOCT^{-1}(Y_k))) \\ &< DCOT(DCOT^{-1}Maxmin(Y_k)) \\ &= Maxmin(Y_k) \end{aligned} \tag{3.30}$$

  – Non-Embedding Domain(Wavelet Domain)

$$\begin{aligned} CollusionAttack_{wavelet}^{maximum} &= DCOT(DWT_{-1}Maxmin(DWT(DOCT^{-1}(Y_k)))) \\ &< DCOT(DWT_{-1}(DWT(DOCT^{-1}Maxmin(Y_k)))) \\ &= Maxmin(Y_k) \end{aligned} \tag{3.31}$$

where $CollusionAttack_{DCOT}^{maxmin}$,$CollusionAttack_{spatial}^{maxmin}$,$CollusionAttack_{wavelet}^{maxmin}$ are the maxmin collusion attack in embedding(DCOT) domain,spatial domain,wavelet domain.Maxmin(.) is the maximum minimum attack perform on fingerprints. The

Equation 3.30,3.31 conclude that maximum attack perform differently in different domains.

$$\mathbf{CollusionAttack}_{\mathbf{DCOT}}^{\mathbf{maxmin}} > \mathbf{CollusionAttack}_{\mathbf{spatial}}^{\mathbf{maxmin}} > \mathbf{CollusionAttack}_{\mathbf{wavelet}}^{\mathbf{maxmin}} \tag{3.32}$$

As random negation attack is combination of minimum and maximum attack ,so Equation 3.23,3.24,3.27,3.28 conclude that random negation attack also has the same performance as the minimum and maximum attack in different domains.

$$\mathbf{CollusionAttack}_{\mathbf{DCOT}}^{\mathbf{rndmneg}} > \mathbf{CollusionAttack}_{\mathbf{spatial}}^{\mathbf{rndmneg}} > \mathbf{CollusionAttack}_{\mathbf{wavelet}}^{\mathbf{rndmneg}} \tag{3.33}$$

- **Median Attack** is ,perform median operation on fingerprints,non linear attack
  - Embedding Domain(DCOT Domain)

$$CollusionAttack_{DCOT}^{median} = Med(Y_k) \tag{3.34}$$

  - Non-Embedding Domain(Spatial Domain)

$$\begin{aligned} CollusionAttack_{spatial}^{median} &= DCOT(Med(DOCT^{-1}(Y_k))) \\ &\approx DCOT((DOCT^{-1}Med(Y_k))) \\ &= (Y_k) \end{aligned} \tag{3.35}$$

  - Non-Embedding Domain(Wavelet Domain)

$$\begin{aligned} CollusionAttack_{wavelet}^{median} &= DCOT(DWT_{-1}Med(DWT(DOCT^{-1}(Y_k)))) \\ &\approx DCOT(DWT_{-1}Med(DWT(DOCT^{-1}(Y_k)))) \\ &= (Y_k) \end{aligned} \tag{3.36}$$

where $CollusionAttack_{DCOT}^{median}$,$CollusionAttack_{spatial}^{median}$,$CollusionAttack_{wavelet}^{median}$ are the median collusion attack in embedding(DCOT) domain,spatial domain,wavelet domain.R(.) is the random negation operation on fingerprints.

- **Modneg Collusion Attack** is,combination of minimum ,maximum and median operation , non linear operation.
  - Embedding Domain(DCOT Domain)

$$CollusionAttack_{DCOT}^{mdneg} = Mdneg(Y_k) \tag{3.37}$$

  - Non-Embedding Domain(Spatial Domain)

$$CollusionAttack_{spatial}^{mdneg} = DCOT(Mdneg(DOCT^{-1}(Y_k))) \tag{3.38}$$

  - Non-Embedding Domain(Wavelet Domain)

$$CollusionAttack_{wavelet}^{mdneg} = DCOT(DWT_{-1}mdneg(DWT(DOCT^{-1}(Y_k)))) \tag{3.39}$$

where $CollusionAttack_{DCOT}^{mdneg}$,$CollusionAttack_{spatial}^{mdneg}$,$CollusionAttack_{wavelet}^{mdneg}$ are the mdneg collusion attack in embedding(DCOT) domain,spatial domain,wavelet

domain.mdneg(.) is the modeneg attack on fingerprints. The Equation 3.27,3.28,3.23,3.24,3.35,3.36 conclude that minimum attack perform differently in different domains.

$$\mathbf{CollusionAttack}_{\mathbf{DCOT}}^{\mathbf{minimum}} > \mathbf{CollusionAttack}_{\mathbf{spatial}}^{\mathbf{minimum}} > \mathbf{CollusionAttack}_{\mathbf{wavelet}}^{\mathbf{minimum}} \tag{3.40}$$

3.5 Conclusion

The chapter focuses on behavior of different literature attack in different embedding and non-embedding domains.Depending upon behavior in domains attack can be divided into three classes. Class-1 have attack which have same effect in different domains. Class-2 have attack with approx same performance in different domains. Class-3 have descending performance in different domains. Class-1 attacks are average attack whereas class-2 attacks are median, maxmin and modneg. Class-3 attacks are minimum, maximum and randneg. Various statistical are driven to prove the correctness of attacks behavior.

Chapter 4

Collusion Resistant Framework with Wave Atom Embedding

4.1 Introduction

Advances in technology comes at cost. The most common example of this is copyright management. The multimedia content over Internet can be attacked and distributed easily as the user can take part remotely. A user can forge multimedia content and redistribute it breaching the copyright law. The most common solution of this is collusion resistant framework. The framework consist of different blocks to resist or detect the illegal distribution.

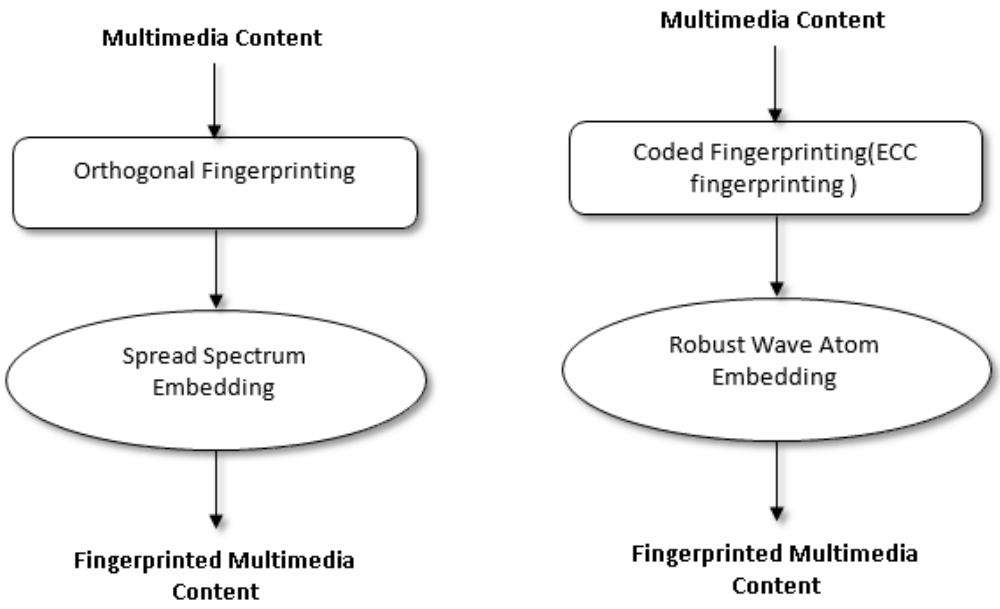
The chapter focuses on defining proposed collusion resistant framework and also discuss the effectiveness of framework. The framework uses error correcting code as base code for fingerprint generation and wave atom transform domain for fingerprint embedding. The main aim of framework is to provide optimal solution to collusion resistant problem.

4.2 Proposed Collusion Resistant Framework

The collusion resistive system proposed here has stem from coded fingerprinting. The coded fingerprint has less collusion resistant whereas high tracing capability. To increase the resistance of framework interleaving embedding scheme [33] used here which intern uses ECC code based on reed solomon code. The framework overcome issues that are existing literature framework. The traditional framework uses orthogonal fingerprints along with spread spectrum embedding. The orthogonal fingerprints has dimensional dependency problem along with it can be easily attacked with various attack[1].

The proposed framework overcome these problem by using modified ECC coded fingerprinting mechanism [33] to generate the fingerprints. The framework uses wave atom embedding [32] for embedding the fingerprints.

Figure 4.1a and 4.1b shows the comparative analysis of framework used in literature and proposed framework.



(a) Conventional Collusion Resistive Framework

(b) Proposed Collusion Resistive Framework

Figure 4.1: Comparison between Proposed and traditional approach

Figure 4.1a shows the block diagram for conventional framework shows that multimedia content is embedded with spread spectrum embedding along with orthogonal fingerprinting mechanism is used for fingerprint generation.

Figure 4.1b shows the block diagram for proposed framework shows that instead of independent fingerprint we use ECC fingerprinting along with robust wave atom embedding to generates the fingerprinted content.

4.2.1 Modified ECC Fingerprinting Mechanism

The ECC fingerprinting mechanism used here is interleaving ECC fingerprint generation which has its stems in block interleaving. The process fallows division of fingerprints into blocks and interchanging them before embedding.

Suppose that generated fingerprints has matrix $F = [f_{jk}]_{L \times N_j}$ such that each element in original fingerprinted are consider as row by row by as interleaving the elements are interleaved and inserted as column by column. The matrix has depth of interleaving N_j,and in original matrix the f_{jk} is jth element of wave atom embedding for kth user's codeword symbol and after interleaving the user corresponding element is $[(k-1)L + j]$. Fingerprint for modified scheme are generated as fallow:

1. Base Code are generated with ECC code generation which fallow Reed-Solomon code over Galois field.

2. The code is divided into sub-blocks.

3. The sub-blocks are rearranged based on secret key.

4. The sub-blocks are combined to form large block.

4.2.2 ECC Fingerprints for Multimedia

The error correcting codes are traceable codes allows high degree for tracing the colluder. The assumption for ECC fingerprints are that marks added by other are treated as error. The hamming distance between the codewords of illegitimate user are much more such that it will not be error. The hamming distance ensures that the matching codewords comes from illegitimate user. The best matching set is denoted by descendant set.The traceable codes are defined as fallows-

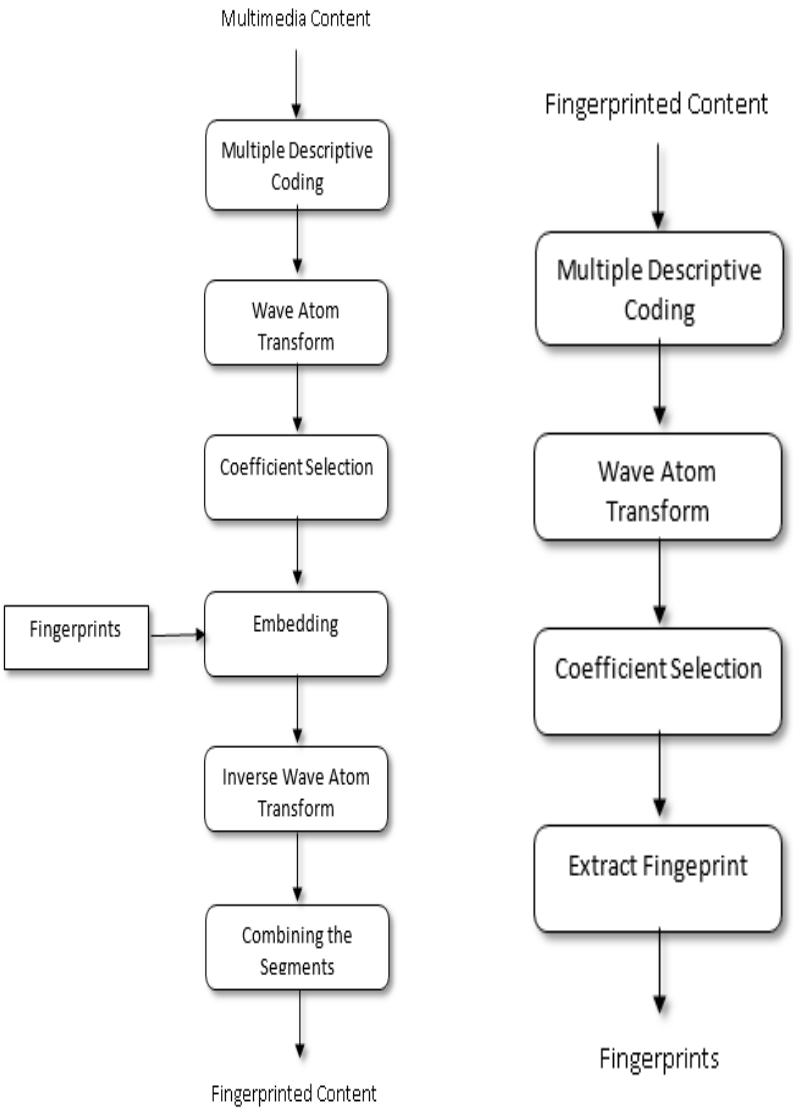
Definition: Let $C \subseteq \sum^N$ be a code of length N with alphabet set $\sum$. The colluder set is represented by $C_s = \{c_1, c_2, c_3, ...c_k\} \subseteq C$ with length k which consist of N marks for every colluder. The $c_1 \epsilon C$ consist of N marks with $c_i = \{c_1^i, c_2^i, c_3^i, ..., c_N^i\}$. The set which has best hamming match with this set is known as descendant set is denoted by $D_s(C_s) = \{(m_1, m_2, m_3, ..., m_N) : m_j \in \{c_j^i : 1 \leq i \leq k\}, 1 \leq j \leq N\}$. For colluder in descendant $(m_1, m_2, m_3, ..., m_N) \in D_S(C_s)$,for any colluder in colluder set $c_i \in C_s$ such that $\mod j : m_j = c_j^{(i)} > \mod j : m_j = u_j^{(i)}$ for legitimate user set $(u_1, u_2, u_3, ..., u_N) \in \sum / C_s$,then the codeword is k-traceability code.

The ECC fingerprint generation fallows reed-solomon code. The reed-solomon code are based on some finite arithmetic field. Codes are linear in nature and stems from BCH codes. Codes are represented with RS(l,m) with q-bit symbols and add parity symbols to make it traceable. The code generated are of length l in which m data symbols are m with q-bit each and rest are parity symbols. The code contains l-m parity blocks with q-bit. A Reed-Solomon code can detect error equals to half of parity bits,so it is d-detectable where 2d = l-m.

4.3 Wave Atom Embedding

The framework proposed here uses wave atom embedding proposed by [33]. Leung uses scheme based on blind watermarking, uses multiple descriptive coding. The scheme intern transform the original multimedia content into wave atom transform domain before embedding watermark. The same scheme is used here for fingerprint embedding with some modification.

Figure 4.2 shows the fingerprint insertion and extraction process for proposed collusion resistant framework. Owner insert the fingerprints into the content. The insertion process is done in wave atom domain which is robust in nature than existing scheme. The fingerprint insertion and extraction are opposite to each other. The suspicious content on receiving



(a) Fingerprint insertion Procedure (b) Fingerprint Extraction Procedure

Figure 4.2: Proposed Collusion Resistive Framework

fallows the extraction procedure to check whether copy is colluded or not. On receiving colluded copy mark of user is checked which has the best match is identified as colluder.

Figure 4.2a shows the insertion procedure for the proposed system.The step are a fallow-

1. Multimedia content is divided into subsegment using multiple descriptive coding.

   Multiple Descriptive Coding: Suppose a multimedia content of size M $N \times N$ is segmented into description as fallow-

$$M_1(i,j) = M(i, 2j-1), M2(i,j) = M(i, 2j)$$

$$M_3(i,j) = M(\frac{N}{2} + i, 2j-1), M4(i,j) = M(\frac{N}{2} + i, 2j)$$

2. Divided subsegment are transformed into wave atom domain.

Wave Atom Transform: Wave atom are replacement of 2-D wavelet which intern obey the parabolic scaling law i.e. $wavelength \approx (diameter)^2$ proposed by Demnanet and Ying [38]. They shown that in wave atoms fingerprints has cover larger space than in other traditional transform domain like curvelets or wavelets.

The elements of boundary of packets $\{\psi_i(x)\}$ where x belong to real domain such that $x \in R^2$, be wave atoms if there exist the constant S_N

$$|\hat{\psi_i}| \leq S_N 2^{-k}(1+2^{-k}|\omega-\omega_i)^{-N}| + S_N 2^{-k}(1+2^{-k}|\omega+\omega_i|)^{-N} \tag{4.1}$$

where $|\psi_i| \leq S_N 2^{-k}(1+2^{-k}|\omega-\omega_i|)^{-N}$ with $N = 1, 2, 3...$ The S_N is constant whose value depends upon environments. The cap over ψ denotes the discrete fourier transform and the subscript $i = (j, l1, l2, n1, n2)$ for a point (x_u, w_u) such that point belongs to phase space- where

$$x_u = (x_1, x_2)_i = 2^{-k}, w_u = (w_1, w_2)_i = \pi 2^k(l1, l2). \tag{4.2}$$

3. The coefficient C_i are being selected from the segment for which coefficient value is larger than certain threshold t.

4. Certain modification is done on selected coefficient to make the system robust is as fallow-

   - Four constant $\beta_a, \beta_b, \beta_c, \beta_d$ and threshold $t1$ is taken depending upon environment.
   - In I_1, I_2
     - In I_1,

       if $abs(C_i) \geq t_1$ **then**
       $C_i = C_i \times \beta_a$
       else
       $C_i = C_i \times \beta_b$
       end if
     - In I_2,

       if $abs(C_i) \geq t_1$ **then**
       $C_i = C_i \times \beta_c$
       else
       $C_i = C_i \times \beta_d$
       end if
   - Similar procedure is fallowed for I_3, I_4

5. Inverse transform is applied on segments to revert back them to original domain.

6. Apply reverse of multiple description coding to collect the four description.

Figure 4.2b shows extraction procedure for fingerprints. The extraction is reverse process of insertion with some changes. The extraction for fingerprinted content is as fallow-

1. The division of content into multiple segment fallows same procedure as insertion.

2. The segments found are transformed into wave atom domain.

3. Coefficient are selected from the obtained subsegment.

4. The coefficient are compared in their even odd subsegment to obtain the fingerprints f_m are as fallow-

$$f_m = \begin{cases} 1, & mean(abs(I_1^{(x)})) > mean(abs(I_2^{(x)})) \\ 0, & mean(abs(I_1^{(x)})) \leq mean(abs(I_2^{(x)})) \end{cases}$$

   where I_1^x and I_2^x are the elements from the odd and even subsegment. The half fingerprint is generated with above step.

5. Similarly the second half of fingerprints is also generated.

4.4 System Design Process

The collusion resistant system some preprocessing before fingerprinting embedding. The detailed system design process is given as fallow-

1. For a given multimedia signal determine the length B and the block size B_s. The alphabet for system is given as a. Then the number of blocks in system $N = \frac{B}{B_s}$

2. Calculate the probability P_{fon} of identifying a wrong mark conspired by at least one conspirator for each of blocks given under robust wave atom embedding.

3. The probability P_{foc} for falsely detecting a mark is calculated by

$$P_{foc} = 1 - p_{fon}$$

4. For an event where number of calculated mark are N_cal is greater than a given number n. The probability of such event E is Binomial distribution over P_{fon}.

$$Pr(E) = Pr(N_cal \geqslant n) = \sum_{N}^{i-n} \binom{N}{i} P_{fon}^{i} (1 - P_{fon})^{N-i} \tag{4.3}$$

5. The probability of event for at least detecting at least one conspirator P_{doc} fallows conditional probability. The limit for P_{doc} is

$$P_{doc} \geqslant Pr(findminimumonecolluder|E)Pr(E) \tag{4.4}$$

Where n = L-Le such that m-traceability code decides Le erasures. The probability for detecting minimum one colluder for given event A is choose to 1. For probability of identifying each colluder P_{d_all} minimum requirement on which system is based ,it is mandate to keep the P_{d_all} is equal or less than event probability. The property of m-TA code[40] has relationship in between which are based on erasures and probability for detecting each colluder. For a given $P_{d_{all}}$ we can calculate m-TA properties like maximum collusion persistence CP_{max} and codeword length to represent the user N_c. Similar computation can fallow to calculate the $P_{d_{all}}$ for given CP_{max} for m-TA code.

4.4.1 Problem Statement

The collusion resistive framework using coded fingerprints are more collusion traceable than collusion resistance. To increase the collusion resistive capacity of framework interleaving scheme is used in which the blocks of fingerprints are interchanged before they are inserted into content.

The non blind detection reduces falsely accusing the user as colluder. The detection procedure fallows extraction of marks and matching the each legitimate user original fingerprints.
For a given user i ,

The T_n statics is-

$$T_n(i) = \frac{(Y_k - M)^T C_{s_j}}{,} i = 1, 2, 3...N_u \tag{4.5}$$

where Y_k is extracted fingerprint for multimedia content M. The C_{s_j} is colluder set and N_u is maximum user for the system can generates the fingeprint.

The collusion resistive capacity is the robustness of system against the conspirator attack. The identification of colluder at max fallows N_u comparison that fallows N_u dimensional codes. The resistive capacity statics for system can calculated by mean,variance and covariance.

The mean-

$$Mean[T_n(i)] = \begin{cases} [\frac{1}{a} + (1 - \frac{1}{a})\sigma]||s||, & a \in C_s \\ \sigma||s||, & a \notin C_s \end{cases} \tag{4.6}$$

The Variance-

$$Variance[T_n(i)] = \begin{cases} [a+1+\sigma(a-1)]\frac{\rho_s^2}{c^2} + \rho_n^2, & i \in C_s \\ (1+\sigma)\frac{\rho_s^2}{c} + \rho_n^2, & j \notin C_s \end{cases} \tag{4.7}$$

Covariance

$$covariance[T_n(i_1), T_n(i_2)] = \sigma\rho_n^2, \qquad n_1 \neq n_2 \tag{4.8}$$

σ is correlation average of two marks. For two user i,j average correlation can be given by

$$\sigma_{ij} = \frac{C_s(i)^T C_s(j)}{||s||} \leq \frac{N-D}{D}$$

where N is code length of Reed-Solomon code with minimum distance D.

In traditional ECC coded fingerprints interleaving attack can be mount by conspirator using detailed comparison and analysis. In modified interleaving ECC code fingerprints significant comparison and analysis is tough as the marks are firstly subdivided into various blocks γ and a permutation among these block is applied before embedding.

4.4.2 Simulation Parameters

Effectiveness of proposed system uses vast amount of parameters.They are as fallow-

- **Interleaving Units:**Number of blocks in which fingerprints are divided. Interleaving operation is performed on the blocks before embedding.
- **Watermark To Noise Ratio:**Ratio of fingerprints and noise in the output image.

  $$WatermarkToNoiseRatio(WNR) = \frac{Y_k}{Noise}$$

  where Y_k is fingerprints for kth user.
- **Quality Factor:**Measure of Image quality degradation during compression process.

4.4.3 Detection Strategies

The main goal of collusion resistive framework is to detect collusion and trace back at least one colluder. The tracing finds the colluder by closely matching the mark to the user. The user with higher correlation is declare as colluder. The detection strategy is as fallow:

1. The wave atom embedding with multiple description [31] allows blind detection because fingerprint can be extracted by comparing the sub blocks.

2. Extracted fingerprint is decoded with ECC decoding algorithm to generate the base code sequence.

3. Comparison is done for extracted sequence with distributed sequence.

4. The user has most matched sequence is identified as colluder.

Various detection strategies are presented in [9], [18] are non-blind detection strategies uses soft and hard detection. As the scheme presented here is blind so these strategies will directly not applicable here.

Detection For Interleaving Attack: Attack involve segmented copies of every colluder to generate the new copy of content. Detection involve extracting the fingerprint and matching it with every fingerprint distributed. The match identify a user as colluder with highest match.

Assume that out of N user C are colluder with colluder set $C_s = \{c_{i_1}, c_{i_2}, c_{i_3}...c_{i_c}\}$. The collusion attack involve C different copies of fingerprinted content $\{C^{(i)}\}_{i=1}^{N}$ to generate a colluded copy with kth component as S_k. Let F_k is extracted fingerprint for kth user.

[18] defines two Gaussian variable for F_1, F_2 which have maximum value for colluder and non-colluder set.

$$F_1 = max_{j \in C_s} F_k, F_2 = max_{j \notin C_s} F_k \tag{4.9}$$

So the mean and variance for F_1, F_2 are as fallow:

$$\begin{aligned} m_{F_1} \cong E[F_1] = \frac{||N||}{L}\left(\frac{L}{c} + \frac{5(c-1(L-D))}{12}\right), \\ \sigma^2_{F_1} \cong Var[F_1] = \frac{||N||}{L}\sigma_c^2 + \sigma_d^2 \end{aligned} \tag{4.10}$$

$$\begin{aligned} m_{F_2} \cong E[F_2] = \frac{||N||}{L} \times \frac{(L-D)+1}{2}, \\ \sigma^2_{F_2} \cong Var[F_2] = \frac{||N||}{L}\sigma_m^2 + \sigma_d^2 \end{aligned} \tag{4.11}$$

$$\begin{aligned} \sigma_m^2 = \left(\frac{(c\,(L-D)-1)}{6}\right)^2, \\ \sigma_d^2 = \left(\frac{5\,(c-1)\,(L-D)}{36}\right)^2 \end{aligned} \tag{4.12}$$

where L is codeword length $D = L - t + 1$ is minimum distance,c is number of colluder. σ_d^2 is additive noise variance.

The probability of detection is:

$$P_d = Pr(F_1 > F_2) = \int_{-\infty}^{+\infty} P(F_1 > th) F_{F_2}(t) dt \tag{4.13}$$

where F_{F_2} is probability distribution function for F_2 and th is certain threshold.

$$P(F1 > th) = -Q\left(\frac{th - m_{F_1}}{\sigma_{F_1}}\right) \tag{4.14}$$

Detection for Average Attack: Attack involve linear operation on copies of colluder. The detection for average attack is as fallow: Let $F_1, F_2, \ldots, F_c$ are the extracted fingerprints from c colluder.Then-

$$\begin{aligned} F &= [F_1, F_2, \ldots, F_u]^T \\ &\approx N\left([m_1, m_2]^T, \sigma_d^2 \sum\right), \\ &\text{where} \\ m1 &= ||F||\left(\frac{1}{c} + \left(1 - \frac{1}{c}\right)\rho\right) 1_c, \\ m2 &= ||F||\rho 1_{N-c} \end{aligned} \tag{4.15}$$

where $||s||$ is fingerprint strength 1_l is a vector of l by 1 with all 1's. $\sum$ is N$\times$ N matrix whose all elements are ρ 's except diagonal element which are 1. m_1 is mean for colluder and m_2 is mean for non colluder.

4.5 Conclusion

The chapter presents the collusion resistive system framework for collusion attack. The chapter discuss the ECC fingerprint generation and wave atom embedding method along with system design process. Various simulation parameters are given for system based on which effectiveness of system is measured along with various detection strategies for attacks.

Chapter 5

Experimental Results and Discussion

Analysis of attacks is root for designing the optimized collusion resistance system. For effectively designing the collusion resistive system it is necessary to know how different attacks behave in different domains. The attacks of same category perform differently in various domains. Chapter 3 presents the scenario and establish various statistical results for same. This chapter presents the experimental result for various collusion attacks in different domains. Depending upon these analysis a robust domain is chosen for efficient collusion resistance system. The chapter also presents various results to show the effectiveness of system.

5.1 Collusion Attacks Analysis

Collusion attack are effectively mount on the multimedia to generate the illegitimate copy. Analysis of attacks in embedding and non-embedding domain is important to know the behavior of attack and to design effective system. Here we presents the analysis of colluder attack model in DCT, spatial, wavelet domain.

5.1.1 Simulation Results

The experiment here investigate the behavior of coded fingerprints in different domain uses standard Lenna image as base image of size 512×512 uses error correcting code(ECC) which uses reed solomon code RS(32,2) over Galois field GF(32). The 9 out of 15 randomly selected fingerprints are selected randomly.

Figure 5.1- 5.6 shows the histogram of image generated in the domains.

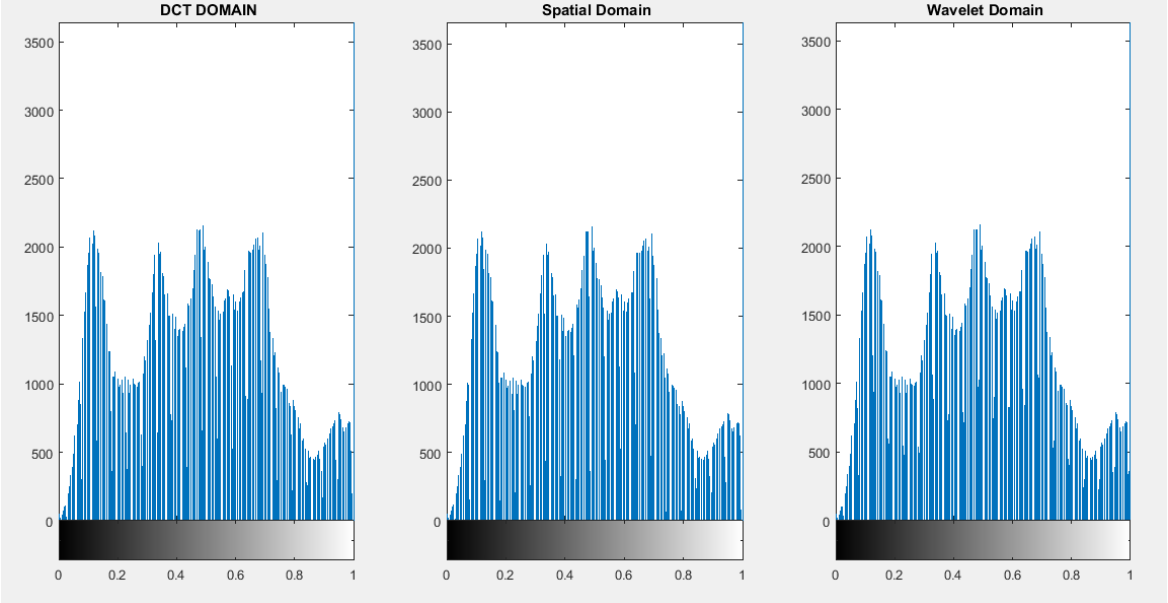


Figure 5.1: Average Collusion Attack in embedding and non-embedding domains

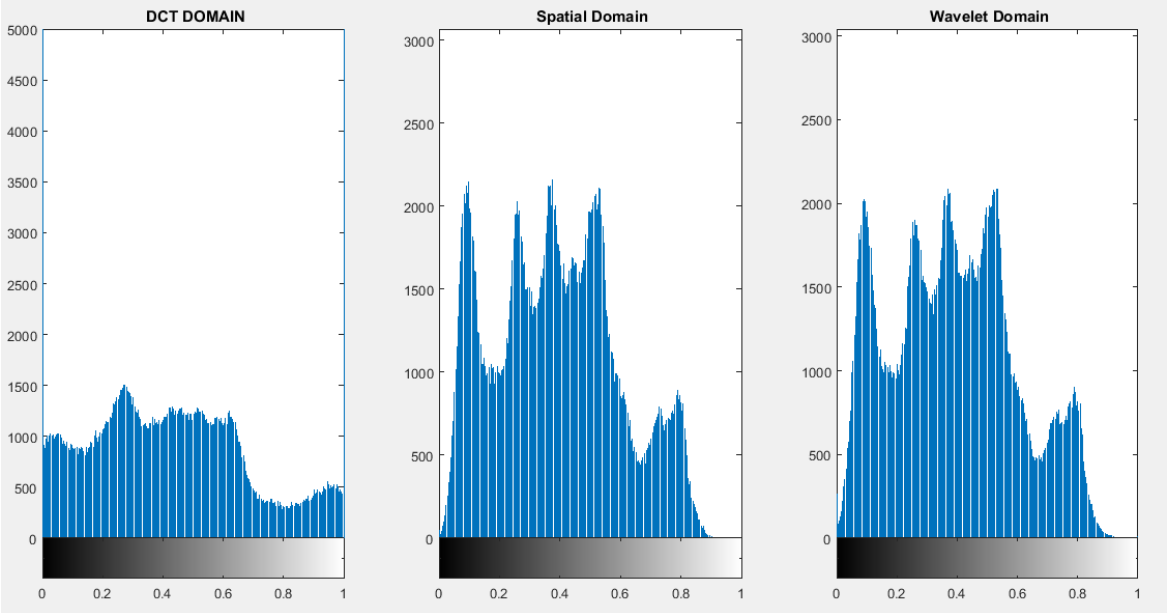


Figure 5.2: Minimum Collusion Attack in embedding and non-embedding domains

- Figure 5.1 shows the histogram of image generated after average collusion is perform over fingerprinted image in domains. As histogram shows they are identical to each other as derived by statistical analysis. Hence the simulation also shows that collusion attack are domain independent.
- Figure 5.2 shows the histogram of image in domains after minimum attack. As histogram are not identical and shows the ascending histogram peak implies minimum attack in embedding(DCT) is most effective and non-embedding(wavelet) is least effective.

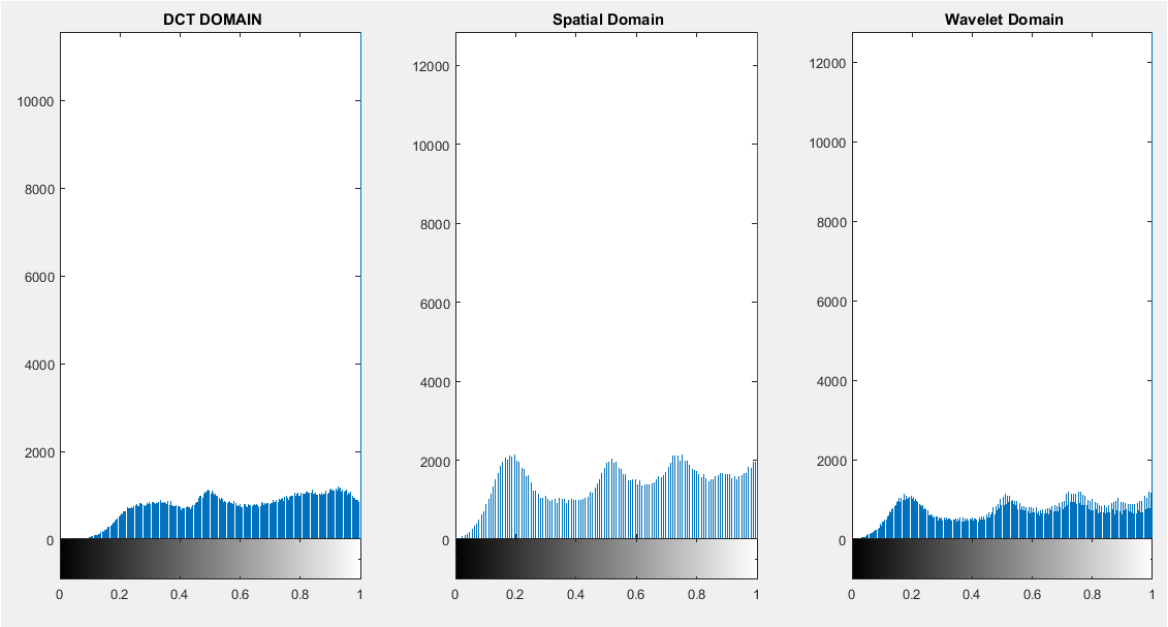


Figure 5.3: Maximum Collusion Attack in embedding and non-embedding domains

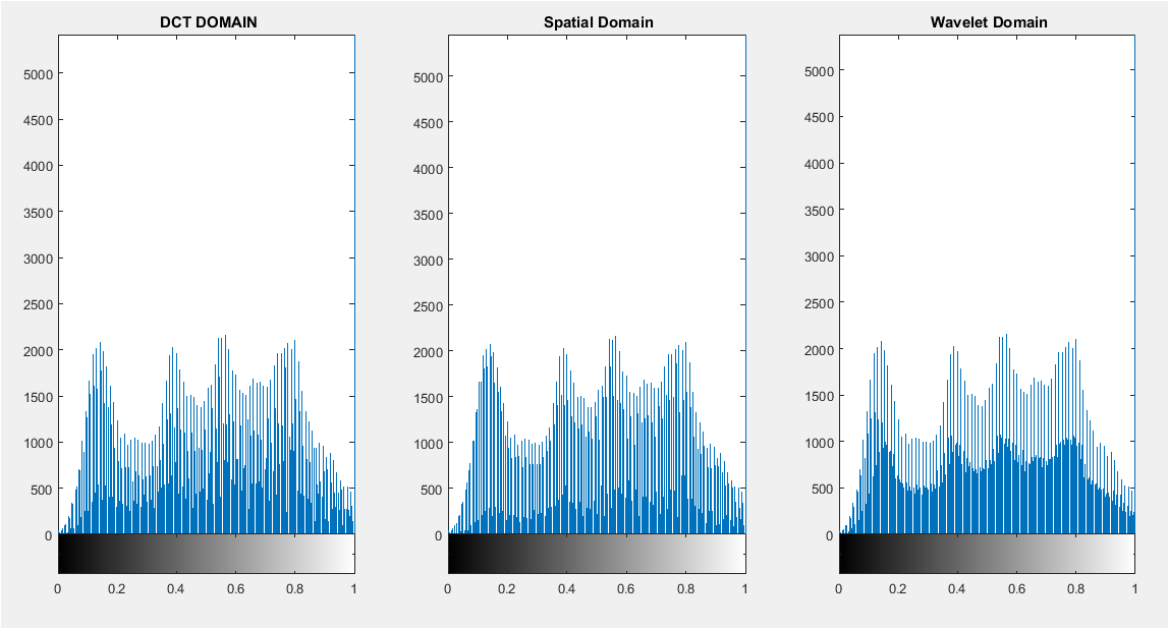


Figure 5.4: Maxmin Collusion Attack in embedding and non-embedding domains

- Figure 5.3 shows the maximum attack scenario in different domains. As the statistical result shows that maximum attack in embedding(DCT) domain is most effective also shown by histogram.Histogram for maximum attack in embedding (DCT) has lowest peak shows effectiveness of attack whereas histogram in non-embedding(wavelet) domain shows highest peak is least effective.

- Figure 5.4 shows the minmax attack scenario in different domains. As the statistical result shows that minmax attack in embedding(DCT) domain is most effective also shown by histogram. Histogram for minmax attack in embedding (DCT) has lowest

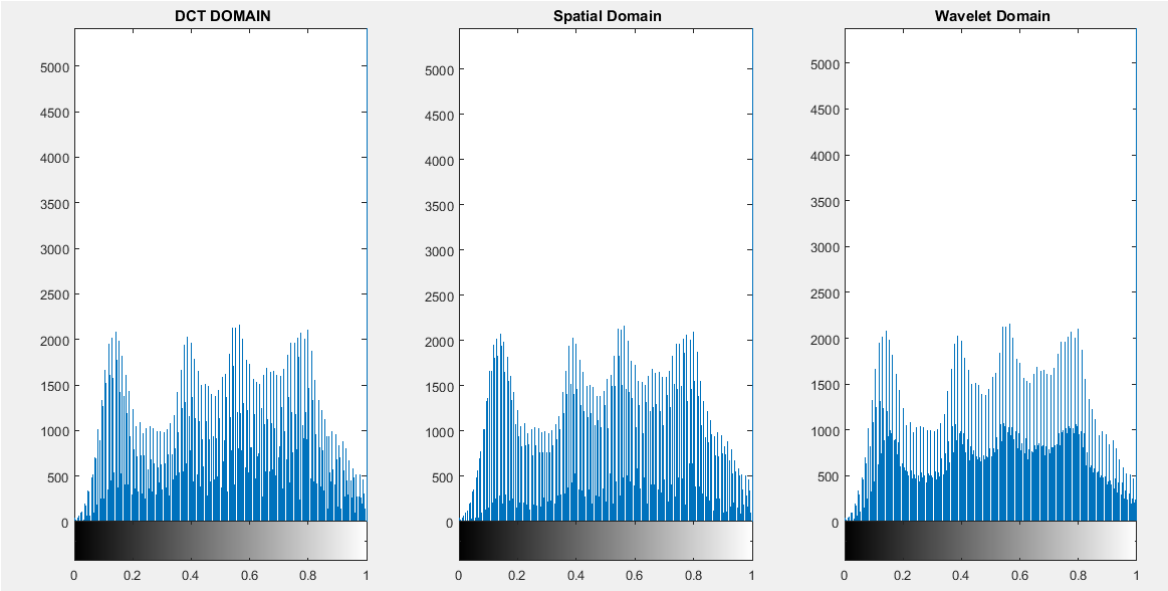


Figure 5.5: Median Collusion Attack in embedding and non-embedding domains

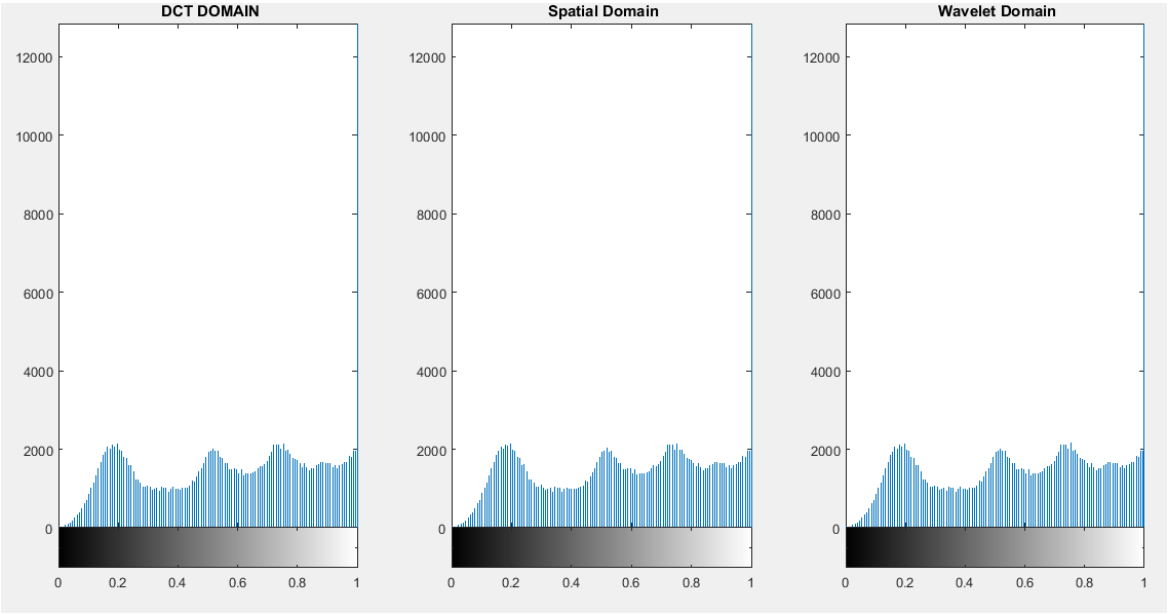


Figure 5.6: Modneg Collusion Attack in embedding and non-embedding domains

peak shows effectiveness of attack whereas histogram in non-embedding(wavelet) domain shows highest peak is least effective.

- Figure 5.5 shows the median attack scenario in different domains. As the statistical result shows that median attack in different domain shows approx same behavior also shown by histogram. Histogram for median attack in embedding (DCT) has almost same histogram as in non-embedding domain.

- Modneg attack shows same behvior as median attack as it is the combination of minimum ,maximum and median attack. Figure 5.6 shows the modneg attack scenario

in different domains. As the statistical result shows that modneg attack in different domain shows approx same behavior also shown by histogram. Histogram for median attack in embedding (DCT) has almost same histogram as in non-embedding domain.

5.2 Proposed Collusion Resistive Framework

The proposed collusion resistance framework uses robust wave atom embedding and ECC fingerprint generation with interleaving. Various results are drawn to show the effectiveness of system as fallow:

5.2.1 Experimental Results

In this subsection, experimental conclusion ae made for the proposed fingerprinted system. The effectiveness of system is measured by detection probability. The detection probability of system is measure against the number of colluder in the system.

Table 5.1: Detection Probability for 200 interleaving units

Number Of Colluder	Watermark to Noise Ratio(in db)			
	0	-5	-10	-15
10	1	1	1	0.9
20	1	1	1	0.76
30	1	1	0.89	0.55
40	1	1	0.70	0.45
50	1	0.92	0.50	0.35
60	1	0.85	0.53	0.25

Table 5.2: Detection Probability for 400 interleaving units

Number Of Colluder	Watermark to Noise Ratio(in db)			
	0	-5	-10	-15
10	1	1	1	1
20	1	1	1	0.64
30	1	1	0.90	0.43
40	1	1	0.85	0.35
50	1	0.9	0.70	0.37
60	1	0.85	0.50	0.38

Table 5.1 and 5.2 showing the detection probability against number of colluder.The two table differs in manner fingerprints generation.

Table 5.1 shows the result for system in which fingerprinting generation uses 200 interleaving units. The table significantly shows the result for mid-high watermark to

noise(WNR) ratio. Results are drawn shows that system perform well for low WNR whereas for high WNR it has low detection probability but perform well against the other existing framework.

Table 5.2 detects the colluder for system with 400 interleaving units. The table showing that it perform well for low WNR whereas for high WNR it detect the colluder with less probability. For 400 interleaving units system perform well than existed system.

The collusion resistive system is tested against two standard multimedia image Lenna and Baboon of size 512×512. The coded fingerprints are based on modified ECC coded marks which is based upon Reed-Solomon code RS(30,2) over GF(32) with 200 interleaving units. For Lenna image the number of embedded blocks $N_l = 37412$, and length of sequence is $N_s = 1240$ and for Baboon $N_l = 87570$ and $N_s = 2919$.

The various quality factor of image also set to check the effectiveness of system. The detection probability of system is checked against quality factor with value 80,60,40 for Lenna and 40,30,20 for Baboon. The quality factor for Lenna corresponds to WNR=1.02 db,-5.06 db,-8.20 db , the same for Baboon corresponds to -7.20 db ,-8.74 db ,-10.53 db. To introduce noise in the system JPEG compression is applied

Various results are drawn for two sample images on the basis of quality factor and watermark to noise ratio.

(a) Standard Lena Image (b) Fingerprinted Lena Image (c) Extracted Fingerprint

Figure 5.7: Framework Output for Lena Image

(a) Standard Baboon Image (b) Fingerprint Baboon Image (c) Extracted Fingerprint

Figure 5.8: Framework Output for Baboon Image

Figure 5.7 and 5.8 shows the various image generated by the system.Figure 5.7 shows the experiments on Lenna image. It shows the standard Lenna image and the fingerprinted image for Lenna and finally the extracted fingerprint for standard image. Figure 5.8 shows the same results for Baboon image.

Table 5.3: Detection Probability for Lenna Image under interleaving attack

Number Of Colluder	Quality Factor(in db)		
	80	60	40
10	1	1	1
20	1	1	1
30	1	1	1
40	1	0.90	0.89
50	1	0.87	0.75
60	1	0.86	0.73

Table 5.4: Detection Probability for Lenna Image under Collusion attack with noise

Number Of Colluder	Quality Factor(in db)		
	80	60	40
10	1	1	1
20	1	1	1
30	1	1	1
40	1	1	0.81
50	1	0.90	0.70
60	1	0.87	0.67

Tables 5.3 and 5.4 shows the experiments on Lenna Image. The detection probability for the system is calculated as function of quality factor and number of colluder.

Table 5.3 shows the detection probability for colluder under interleaving attack. The table shows that system performed well for image with high quality factor whereas its performance degrades under low quality factor. In spite of low quality factor system has high detection capability for Lenna Image.

Table 5.4 shows the system probability for catching colluder under average attack. To check the system effectiveness attack fallows image compression attack to introduce noise in system. The system has high detection probability under collusion attack as well.

Tables 5.5 and 5.6 shows the experiments on Baboon Image. The detection probability for the system is calculated as function of quality factor and number of colluder.

Table 5.5 shows the detection probability for colluder under interleaving attack. The table shows that system performed well for image with high quality factor whereas its performance degrades under low quality factor. In spite of low quality factor system has high detection capability for Baboon Image.

Table 5.5: Detection Probability for Baboon Image under interleaving attack

Number Of Colluder	Quality Factor(in db)		
	40	30	20
10	1	1	1
20	1	1	1
30	1	1	1
40	1	1	0.92
50	1	1	0.80
60	1	0.90	0.60

Table 5.6: Detection Probability for Baboon Image under Collusion attack with noise

Number Of Colluder	Quality Factor(in db)		
	80	60	40
10	1	1	1
20	1	1	1
30	1	1	0.93
40	1	1	0.90
50	1	1	0.73
60	1	0.98	0.70

Table 5.6 shows the system probability for catching colluder under average attack. To check the system effectiveness attack fallows image compression attack to introduce noise in system. The system has high detection probability under collusion attack as well.

Table 5.7: Comparison of fingerprint extraction and insertion

Fingerprinting Scheme	Embedding Time(seconds)	Extraction Time(seconds)
Leung et al.[33]	6.41	5.37
Tao et. al.[39]	0.9	9.45
Xaio et.al.[40]	6.22	2.31
Cheng et. al.[32]	2.43	0.32
Proposed Scheme	3.30	2.23

Table 5.7 shows the comparison results for various literature and proposed scheme. The table shows the fingerprint embedding and extraction time for various scheme. The table shows that the scheme has significant less insertion time than the existing schemes.The system also outperform in extraction time except the *Cheng et al.* [32].

5.3 Discussion

Role of Multiple Description Coding(MDC): The multiple description is preprocessing for framework to make it suitable for embedding . It divides the original content into sub

blocks or description. There are two benefits of using MDC -(1)it simplifies the embedding process as now the content to process is one fourth as before.(2)It allows Blind detection of fingerprints[33].

Role of Wave Atom Embedding : The embedding domain make it hard for colluder to extract the fingerprints. The wave atom transform domain is robust against variety of image processing attack like removal of fingerprints[33].

Role of Interleaving ECC Coding:A ECC code is more traceble than collusion resistive, but with modified ECC it is much more collusion restive for high watermark to noise ratio. The interleaving applied on the sub block of fingerprints before applying it to content according to certain key which makes it more collusion resistive[31].

5.4 Conclusion

The chapter present here various results for proposed collusion resistive framework and also for analysis of different collusion attack. The results for collusion attacks justifies various statistical results of chapter 3. The results of proposed framework proves the effectiveness of system against two most popular attack.

Chapter 6

Conclusion and Future Work

In this thesis work, the problem of collusion attack over multimedia content has been addressed. After a deep analysis of the already existing research work in this area, robust wave atom embedding based collusion resistive framework has been proposed here in order to resist the collusion attack. First, a detail analysis of various collusion attack in different domains is provided which is basis of designing the effective collusion resistive system. Here, analysis of attack in embedding and non-embedding domains is provided. The embedding domain is mainly DCT domains whereas non-embedding domains are wavelet and spatial domains. The framework presented here consider both fingerprint generation and embedding. Fingerprints generation fallows ECC fingerprinting mechanism along with interleaving and embedding fallows wave atom embedding. For the proposed framework, it can be seen that it is highly collusion resistive . Fingerprint generation and embedding guarantees both resistance and tracing in the system. The fingerprint embedding mechanism for framework is quite robust in nature such that it can tackle with common image processing attack to remove certain part of image.

While conducting the simulations, the results are limited to multimedia images. For further research, an extension of proposed scheme to resist the collusion attacks in various multimedia content should be taken into consideration. The insertion process time for framework is also a point of interest in future.

References

[1] Y. Wu, "Linear combination collusion attack and its application on an anti-collusion fingerprinting." in *ICASSP (2)*, 2005, pp. 13–16.

[2] D. Boneh and J. Shaw, "Collusion-secure fingerprinting for digital data," *Information Theory, IEEE Transactions on*, vol. 44, no. 5, pp. 1897–1905, 1998.

[3] M. Wu, W. Trappe, Z. J. Wang, and K. Liu, "Collusion-resistant fingerprinting for multimedia," *Signal Processing Magazine, IEEE*, vol. 21, no. 2, pp. 15–27, 2004.

[4] I. J. Cox, J. Kilian, T. Leighton, and T. Shamoon, "A secure, robust watermark for multimedia," in *Information Hiding*. Springer, 1996, pp. 185–206.

[5] W.-G. Kim and Y. Suh, "Short n-secure fingerprinting code for image," in *Image Processing, 2004. ICIP'04. 2004 International Conference on*, vol. 4. IEEE, 2004, pp. 2167–2170.

[6] B. Chor, A. Fiat, M. Naor, and B. Pinkas, "Tracing traitors," *IEEE Transactions on Information Theory*, vol. 46, no. 3, pp. 893–910, May 2000.

[7] A. Fiat and T. Tassa, "Dynamic traitor tracing," *Journal of Cryptology*, vol. 14, no. 3, pp. 211–223, 2001.

[8] H. V. Zhao, M. Wu, Z. J. Wang, and K. Liu, "Forensic analysis of nonlinear collusion attacks for multimedia fingerprinting," *Image Processing, IEEE Transactions on*, vol. 14, no. 5, pp. 646–661, 2005.

[9] D. Schonberg and D. Kirovski, "Fingerprinting and forensic analysis of multimedia," in *Proceedings of the 12th annual ACM international conference on Multimedia*. ACM, 2004, pp. 788–795.

[10] G. Caronni, "Assuring ownership rights for digital images," in *Verläßliche IT-Systeme*. Springer, 1995, pp. 251–263.

[11] D. Kundur and K. Karthik, "Video fingerprinting and encryption principles for digital rights management," *Proceedings of the IEEE*, vol. 92, no. 6, pp. 918–932, 2004.

[12] Z. J. Wang, M. Wu, H. V. Zhao, W. Trappe, and K. Liu, "Anti-collusion forensics of multimedia fingerprinting using orthogonal modulation," *Image Processing, IEEE Transactions on*, vol. 14, no. 6, pp. 804–821, 2005.

[13] S. Lian and Z. Wang, "Collusion-traceable secure multimedia distribution based on controllable modulation," *Circuits and Systems for Video Technology, IEEE Transactions on*, vol. 18, no. 10, pp. 1462–1467, 2008.

[14] W. Trappe, M. Wu, Z. J. Wang, and K. Liu, "Anti-collusion fingerprinting for multimedia," *Signal Processing, IEEE Transactions on*, vol. 51, no. 4, pp. 1069–1087, 2003.

[15] A. Barg, G. R. Blakley, and G. A. Kabatiansky, "Digital fingerprinting codes: problem statements, constructions, identification of traitors," *Information Theory, IEEE Transactions on*, vol. 49, no. 4, pp. 852–865, 2003.

[16] I. J. Cox, J. Kilian, F. T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia," *Image Processing, IEEE Transactions on*, vol. 6, no. 12, pp. 1673–1687, 1997.

[17] A. A. Manaf, A. Boroujerdizade, and S. M. Mousavi, "Collusion-resistant digital video watermarking for copyright protection application," *International Journal of Applied Engineering Research*, vol. 11, no. 5, pp. 3484–3495, 2016.

[18] S. He and M. Wu, "Collusion-resistant video fingerprinting for large user group," *Information Forensics and Security, IEEE Transactions on*, vol. 2, no. 4, pp. 697–709, 2007.

[19] M. Kuribayashi, "Hierarchical spread spectrum fingerprinting scheme based on the cdma technique," *EURASIP Journal on Information Security*, 2011.

[20] M. D. Munoz-Hernandez, J. J. Garcia-Hernandez, and M. Morales-Sandoval, "A collusion-resistant fingerprinting system for restricted distribution of digital documents," *PloS one*, vol. 8, no. 12, p. e81976, 2013.

[21] B.-H. Cha and S.-I. Choi, "Continuous media fingerprinting against time-varying collusion attacks," *Information Sciences*, vol. 298, pp. 66–79, 2015.

[22] A. Qureshi, D. Megías, and H. Rifà-Pous, "Framework for preserving security and privacy in peer-to-peer content distribution systems," *Expert Systems with Applications*, vol. 42, no. 3, pp. 1391–1408, 2015.

[23] H. Zhao, M. Wu, Z. J. Wang, and K. Liu, "Nonlinear collusion attacks on independent fingerprints for multimedia," in *Acoustics, Speech, and Signal Processing, 2003. Proceedings.(ICASSP'03). 2003 IEEE International Conference on*, vol. 5. IEEE, 2003, pp. V–664.

[24] X.-W. Li, B.-L. Guo, X.-X. Wu, and L.-D. Li, "On collusion attack for digital fingerprinting," *Journal of Information Hiding and Multimedia Signal Processing*, vol. 2, no. 4, pp. 366–376, 2011.

[25] H. V. Zhao, M. Wu, Z. J. Wang, and K. Liu, "Forensic analysis of nonlinear collusion attacks for multimedia fingerprinting," *Image Processing, IEEE Transactions on*, vol. 14, no. 5, pp. 646–661, 2005.

[26] G. Doerr and J.-L. Dugelay, "New intra-video collusion attack using mosaicing," in *Multimedia and Expo, 2003. ICME'03. Proceedings. 2003 International Conference on*, vol. 2. IEEE, 2003, pp. II–505.

[27] D. Kirovski and M. K. Mihçak, "Bounded gaussian fingerprints and the gradient collusion attack [multimedia fingerprinting applications]," in *Acoustics, Speech, and Signal Processing, 2005. Proceedings.(ICASSP'05). IEEE International Conference on*, vol. 2. IEEE, 2005, pp. ii–1037.

[28] Y. Wu, "Nonlinear collusion attack on a watermarking scheme for buyer authentication," *Multimedia, IEEE Transactions on*, vol. 8, no. 3, pp. 626–629, 2006.

[29] J. Etesami and N. Kiyavash, "A novel collusion attack on finite alphabet digital fingerprinting systems," in *Information Theory (ISIT), 2014 IEEE International Symposium on*. IEEE, 2014, pp. 2237–2241.

[30] H. G. Schaathun, "Attacks on kuribayashi's fingerprinting scheme." *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 4, pp. 607–609, 2014.

[31] X. Zheng, A. Zhang, S. Li, B. Jin, and J. Tang, "Interleaving embedding scheme for ecc-based multimedia fingerprinting," in *Digital Watermarking*. Springer, 2010, pp. 211–223.

[32] M. Cheng and Y. Miao, "On anti-collusion codes and detection algorithms for multimedia fingerprinting," *Information Theory, IEEE Transactions on*, vol. 57, no. 7, pp. 4843–4851, 2011.

[33] H. Leung and L. Cheng, "Robust blind watermarking scheme using wave atoms," in *Digital Watermarking*. Springer, 2010, pp. 148–158.

[34] M. Koubaa, M. Elarbi, C. B. Amar, and H. Nicolas, "Collusion, mpeg4 compression and frame dropping resistant video watermarking," *Multimedia Tools and Applications*, vol. 56, no. 2, pp. 281–301, 2012.

[35] A. Boroujerdizadeh, A. Ghobadi, A. Yaribakht, and M. Shahidan Bin Abdoullah, "A novel method to reduce collusion attack possibility on watermarking," in *Advanced Communication Technology (ICACT), 2013 15th International Conference on*. IEEE, 2013, pp. 1066–1071.

[36] A. Z. Tirkel, T. E. Hall, C. F. Osborne, N. Meinhold, and O. Moreno, "Collusion resistant fingerprinting of digital audio," in *Proceedings of the 4th international conference on Security of information and networks*. ACM, 2011, pp. 5–12.

[37] S. Maity, J. Sil, S. P. Maity, and C. Delpha, "Optimized spread spectrum watermarking for fading-like collusion attack," in *Wireless Personal Multimedia Communications (WPMC), 2011 14th International Symposium on*. IEEE, 2011, pp. 1–5.

[38] L. Demanet and L. Ying, "Wave atoms and time upscaling of wave equations," *Numerische Mathematik*, vol. 113, no. 1, pp. 1–71, 2009.

[39] P. Tao and A. M. Eskicioglu, "A robust multiple watermarking scheme in the discrete wavelet transform domain," in *Optics East*. International Society for Optics and Photonics, 2004, pp. 133–144.

[40] Y. Xiao, L.-M. Cheng, and L. Cheng, "A robust image watermarking scheme based on a novel hvs model in curvelet domain," in *Intelligent Information Hiding and Multimedia Signal Processing, 2008. IIHMSP'08 International Conference on*. IEEE, 2008, pp. 343–347.

Dissemination

Journal Articles

1. Deepak Shukla,Ruchira Naskar,"Collusion Resistive Framework for Multimedia Security",Frontier of Computer Science,Springer(In Communication).